Asociación Española de Banca

EBA consultation on DRAFT RECOMMENDATIONS ON OUTSOURCING TO CLOUD SERVICE PROVIDERS

24July 2017

Introductory remarks

We welcome the initiative from EBA to set up recommendations regarding the outsourcing to cloud service providers, as the adoption of cloud services by financial institutions is in clear need of regulatory and supervisory certainty. In addition to our specific responses to the questions of this Consultation, we would like to remark the following aspects:

- The lack of harmonisation in regulatory approaches across different jurisdictions and the lack of clarity in supervisory expectations have hindered the adoption of cloud services. The framework of outsourcing to cloud services needs to be complete, transparent and homogenous in the EU. The instrument used by the EBA, which is recommendations that by nature are not directly applicable and not mandatory in a first instance, might not achieve the look-for harmonization, especially because of the different interpretations that may be adopted by national competent Authorities hereafter.

- Nowadays in the market there are few leading cloud services providers so it implies a limited possibility of negotiation of contracts: there are terms that are *adherence clauses.* These recommendations may help financial institutions in these negotiations but still cloud service providers´ concessions may be narrow in the future. The cloud is an important element for financial services to offer an appropriate service in the digital age for consumers and to afford a real digital transformation. The possibility of asking for some type of requirements directly to service providers should be considered. A EU system of official internationally recognized certifications or set of requirements for cloud service providers in financial services should be explored for this purpose.

- As long as cloud is not only used by banks, other entities either from the financial sector or from different sectors should be subject to similar recommendations. The rules applicable should be the same to avoid risks and allowing a level playing field between companies using the same kind of data.

1. Are the provisions of these recommendations clearly and sufficiently detailed to be used in the context of cloud outsourcing?

We welcome EBA's efforts to harmonize cloud outsourcing criteria and interpretations. The principle and risk-based approach and the proportionality considerations seem adequate.

Additionally, the proposed flexibility seems convenient to accommodate the new challenges and ensure these recommendations are future-proof.

However, as already mentioned before, if one of the purposes of these recommendations was to bring harmonization and avoid national regulatory and supervisory divergences, technical standards or any other instruments which is directly applicable would have been a better option.

With the adoption of recommendations, national divergences could take place. For instance, the recommendations include a non-exhaustive list of general criteria, therefore allowing national competent Authorities to include their own additional criteria or to have different interpretations on how to fulfil the proposed requirements. For this particular case, and to avoid a potential lack of harmonization, we understand that the list of criteria should be exhaustive and does not leave much room for interpretation.

It is also relevant to mention that it should be perfectly clear that neither these EBA recommendations on cloud, nor any EU supervisory framework applies to cloud outsourcing by financial institutions that are not subject to the EU supervisory framework even though the parent company is under it. Instead, outsourcing by financial entities that are not in the EU must be ruled by local outsourcing and data protection rules.

Please find below our comments to the specific areas:

4.1 Materiality Assessment

Despite a definition of materiality being provided, draft recommendations do not give any qualitative or quantitative criteria to objectively establish if a service is considered material or not. For the sake of harmonization and legal certainty, the recommendations should set relative and absolute terms to evaluate the materiality of a service (e.g. quantity/quality, typology of the service).

Additionally, among the four criteria indicated, only the one related to the criticality and inherent risk profile of activities to be outsourced is specific to cloud outsourcing. On the contrary, the rest of criteria to be taken into account have to be assessed in any service, even on those directly offered without any outsourcing agreement.

Recommendations should also clearly establish that materiality needs to be assessed at a standalone basis, by entity, not at a group level. Each subsidiary should perform its materiality assessments.

We also suggest that the recommendations recognize automatically as non- material the test environments without real data or with anonymized data, avoiding the assessment prior to outsourcing in those cases.

Finally, it should not be necessary to notify the provision of any other service within a contract already assessed by the National Competent Authority. This contract with a CSP should have been previously notified by the Financial Institution along with the underlying security conditions.

In the same line, recommendations should indicate the possibility of avoiding double assessment in cases where the activity is identical or very similar. It should be possible to rely on previous similar assessments. In cases where a different aspect should be considered the assessment should only cover divergent points. Moreover, when adding an activity into a frame contract with the same or very alike objective there may be cases where the assessment may not be necessary.

4.2 Duty to adequately inform supervisors

This recommendation does not establish precisely what should be communicated to the Authority/Authorities (national and/or ECB level) nor the procedure and deadline for Authorities to accept/not oppose the outsourcing of the service.

As already mentioned, it is key that the recommendations cover the cases in which an authorization can be required and those where a communication to the authority should be enough (such as internal data of employees; c.v., training, etc.) to avoid divergent approaches in different jurisdictions. Recommendations should indicate the **maximum days that an authority may require responding about a cloud outsourcing authorization**. In this scope, a certification recognized by the authorities may facilitate the process and provide assurance.

We believe that the communication of contractual agreements with Cloud Service Providers (CSPs) once signed - and the security policy and criteria agreed by the financial institution and the CSP - should be enough. Once the national Competent Authority has reviewed and validated the underlying conditions and obligations, it should not be necessary to notify the provision of any service within this already assessed framework.

In relation to information to be made available to competent Authorities, in bullet (c) it is required informing the "*country where the service is performed (including location of data)*". However, physical access to data is not coherent with the distributed nature of cloud services. Thus, these recommendations should focus on ensuring access to data from the geography of the outsourcing financial institution and not on location of data, that is already regulated by applicable data protection regulations.

For financial institutions, it is very difficult to comply with timing conditions required by some EU member states legislation, as it is the case with Spanish Circular 2/2016 that requires Financial Institutions to notify the outsourcing one month before the initiative is

in production. Moreover, timing requirements are not harmonized at EU level. In this respect, we consider the process should allow the communication to take place once the cloud initiative is in the production phase.
Regarding the obligation of keeping a record of non-material outsourced activities, we consider that complying with this requirement would be burdensome and costly without providing a clear added value. Thus, the updated register should cover only the relevant and material outsourced activities.

It is necessary to clarify in these recommendations that in case of company groups this register can be developed at entity level according with its internal governance system. **Therefore, each subsidiary may maintain its register according to its idiosyncrasy.**

4.3 Access and Audit rights and 4.4 in particular for the right of access

It must be taken into consideration that for CSPs having a high number of financial institutions as customers would be very difficult to assist auditors appointed by each of their customers, as this continuous affluence of auditors could disrupt their activities.

Moreover, given the nature of cloud services, having access to the data centre where data are located is an unattainable requirement, since data are usually distributed and replicated among different data centres.

Because of that, the EBA should consider including in section 4.3 dispositions ensuring that virtual access to data, with continuous monitoring capabilities for the outsourcing institution, is granted to outsourcing institutions and competent authorities. Otherwise, these recommendations are at risk of soon becoming irrelevant in practical terms.

Regarding the audit right it is complicated and burdensome in order to ensure an effective performance of the cloud service provider. The use of certifications should be considered to facilitate the execution of this right used by clients in business as usual situations (i.e. SSAE 16 y ISAE 3402. ISO XXX, etc.).

4.5 Security of data and systems.

This section properly recognizes the need that CSPs comply with contractual arrangements regarding security terms, especially those related to confidentiality, privacy, data protection and cybersecurity. It is very welcomed the idea that the adoption of cloud solutions by financial institutions has to come hand-to-hand with CSPs' obligation to deliver all the security measures required by the former. Notwithstanding, for further information on this section, see our response to question 2.

4.7 Chain outsourcing

Paragraph 21 sets that "*SP should be obliged to inform the outsourcing institution on any proposed significant changes which may affect the ability of the service provider to meet its responsibilities under the outsourcing agreement*". From our point of view, the term "significant" is vague and open to interpretation. To ensure a harmonized approach, EBA should issue some guidance on the criteria to be considered when assessing the impact of a change.

In paragraph 23 it is stated that "*the notification period for those changes should be contractually pre-agreed to allow the outsourcing institution to carry out a risk assessment to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect*", but it is not clear if this risk assessment is optional for the outsourcing institution or, on the contrary, if there is an obligation for the outsourcing institution to perform this new risk assessment.

In our view, the cloud service provider should be the one to conduct the due diligence, risk assessments, controls and checks to assure that all the subcontractors have the security warranties to comply with what is agreed on the contract. In practice, it is extremely difficult for financial institutions to have control on the whole outsourcing chain. If the cloud service provider changes of subcontractor, the due diligence should be conducted by the cloud service provider. What the client does with the provider, the providers should perform with their providers.

It could be appropriate to include an early termination clause to perform in case the outsourcing institution does not agree with the appointment of a new sub-contractor.

The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution on any proposed significant changes to the subcontractors or the subcontracted services named in the initial agreement, which may affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period for those changes should be contractually pre-agreed and informing about the risk-assessment and due-diligence conducted to allow the outsourcing institution to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect and to conduct a review, if needed, and apply an early termination clause in case the outsourcing institution does not agree with that appointment.

4.8 Contingency plans and exit strategies.

There may be cases in which the continuity of a type of service may not be assured but if it is identified, controlled and covered with other services it should be considered acceptable. Nowadays not all services can be replaced as in the new digital environment there are services only provided by one supplier, therefore the continuity of the same type of service

could be impossible. However, the financial institutions may not be outside of these new products and services (e.g. those based in AI).

27. An outsourcing institution should also ensure that they are ***able to exit*** *cloud outsourcing arrangements if needed.* ~~*without undue disruption to their provision of services, or adverse effects on their compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients.*~~

Moreover, we suggest differentiating regulatory and supervisory expectations for *contingency planning* referring to the exit to other providers or inwards (back to internal infrastructures). We fully agree with exit to other providers having to be ensured by contractual arrangements. However, it is very difficult in practice to ensure exit to internal infrastructures, and this should be considered by both the EBA and national competent authorities. Therefore, paragraph 27.c) should be amended as follows:

"(c) Ensure the outsourcing agreement includes an obligation on the cloud service provider to orderly transfer the activity and that of the subcontractors to another service provider ~~*or to the direct management of the outsourcing institution*~~ *in case of the termination of the outsourcing agreement.*

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

Two main challenges arise when negotiating contract arrangements with CSPs: (i) CSPs reluctance or inability to assume contract terms in practice (e.g. user's and supervisor's right to audit), and (ii) CSP are not always willing neither to negotiate their template contracts to accommodate to different regulations and national or entity specificities nor to include non-regulated issues into contractual arrangements. The position CSPs is adopting in contractual negotiations arise from the fact that they are not required to comply with the banking regulatory and supervisory rules.

For instance, financial institutions are required to ensure in their outsourcing contracts that competent Authorities can access and audit CSPs in relation to Financial Institutions' activities and can take control of the contract in an event related with the Recovery and Resolution Directive.

Given that introducing these requirements in contracts with CSPs, whose services are not only offered to financial Institutions, is usually a burdensome battle for financial institutions, the creation of a mechanism that guarantees that CSPs are aware of the requirements above and accept them, would ease the negotiation with CSPs and foster cloud adoption.

Therefore, it would be of great value for the financial industry that a common set of minimum requirements to be promoted at EU level, translated into a core of minimum contractual arrangements between CSPs and their users. Some of them could be:

- That CSPs allow their users to undertake every operational or technological controls required by internal policies, processes and governance arrangements, as well as every requirement regulators or supervisors may ask in the future.
- That CSPs comply with all EU data protection and privacy rules.
- That CSPs obtain and maintain every certification required by specific regulator or body governing cloud computing services. In this respect, it would be useful to adopt a single certification scheme at EU level, which all CSPs should obtain to be able to provide cloud services to the financial sector.
- That CSPs ensure cloud users to undertake continuous monitoring activities whenever necessary, as well as virtual or ongoing audit.
- That CSPs must report any IT or cybersecurity incident, in particular when the data breach could be identified as that pertaining to a specific client, to both their clients and their supervisors, and that they will ensure that incident reporting deadlines are met by their clients. For example, the 2-hour deadline for the initial reporting of incidents under the EBAs consulted Guidelines on major incident reporting under PSD2 will not be met by banks if contractual arrangements do not oblige CSPs to either report the incidents to the supervisors by themselves or report to their client with sufficient time in advance.
- That CSPs have a business continuity plan for every client, to ensure the latter are able to switch providers whenever they deem necessary.
- That users of cloud computing services hold the right to extract data at any time.

Moreover, this mechanism could also foresee the possibility of the CSP requiring a prior review by Authorities, whose outcome would be an opinion on their capacities and adequacy to financial regulation for different types of services. In case that a financial institution intends to outsource an activity that falls into a type of service to which Authorities have issued a positive opinion, this outsourcing could benefit from a "fast-track" notification/authorization procedure.

We believe that if this mechanism (e.g. voluntary CSPs certification) were offered in an optional basis and CSPs can voluntarily have recourse to it, no changes on the regulatory framework applicable to CSPs and financial institutions would be needed.

On the other hand, if Authorities identify CSPs whose capacities do not allow the outsourcing companies to comply with applicable financial regulation, their inclusion on a public blacklist of non-compliant CSPs would be very helpful for outsourcing companies.