Dear Sir/Madam,

Standard Chartered Response to the European Banking Authority’s (EBA) consultation paper EBA/CP/2017/06 on Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010

Standard Chartered welcomes the publication of the EBA’s draft recommendations on outsourcing to cloud service providers (CSPs) and the opportunity to provide comments to the consultation.

Cloud computing has become integral within the banking sector offering large-scale and cost-effective solutions for data storage, efficient processing, lowered IT costs, and permitting greater flexibility alongside shorter product development timelines.

Common among other technological advancements, it is unclear how banks can fully optimise cloud services given the lack of clarity in the current regulatory landscape. There are risks associated with the growth of outsourcing of cloud computing, including possible concentration of risk among larger CSPs along with concerns around data protection and security. Given the importance of cloud computing to the banking sector, as well as the emerging risks posed by the widespread use of outsourcing, it is crucial that a robust framework is in place for outsourcing agreements for CSPs. In this context, the EBA’s consultation to provide clarity is helpful.

We agree with the EBA that the current framework addressing the process of outsourcing does not adequately provide certainty with regards to the process of outsourcing to cloud service providers and should be tailored to the specificities of cloud outsourcing. Regulatory practices covering outsourcing to CSPs vary across jurisdictions, and we welcome the EBA’s efforts to promote harmonisation and greater consistency across the European Union, as well as with other jurisdictions.

In general, with regards to audit provision and its intended purpose with respect to CSPs, one of the reasons CSPs do not permit access to data centres is because of their security requirements, and given the nature of this industry there often may not be much information to gain from direct access to a physical centre. As such, it might be more helpful to the outsourcing institution if CSPs demonstrate that their processes were properly performing their roles, for example in systems operations centres, instead of focusing on the specifics of negotiating contractual terms, notice periods and fees. This may be more beneficial and result in a better outcome in terms of security. For instance, CSPs could be required to have their own audits, covering specific issues identified by and agreed across regulators, which would then be disclosed to all their clients and regulators.

Although outsourcing to CSPs may raise questions around security, most CSPs have robust security and data management frameworks in place that are often well advanced of financial institutions, which may result in a reduction of risk for some outsourcing institutions. It is important that requirements imposed on CSPs reflect the positive role CSPs can perform in reducing risk, rather than just considering them a possible source of greater risk.
The recommendations provided in the EBA’s consultation paper are helpful. However, additional clarity would be useful in a number of important areas for the industry:

- **Access and audit rights:** Greater clarity on the limitations on audit rights would be beneficial, especially in terms of providing more structure on when the effective exercise of the rights of access and audit would be considered impeded or limited by contractual arrangements.

- **Security requirements:** The security recommendations presented in the consultation may not be sufficient in certain areas. Greater clarity and detail on information security requirements for CSPs in particular would be welcome.

- **Materiality assessment:** The consultation outlines recommendations that would apply equally to both Material and Non-Material Outsourcing. Differentiating requirements based on materiality would be helpful in ensuring a proportionate approach, such as by clarifying different approaches in relation to audit and chain outsourcing for Material versus Non-Material Outsourcing.

In addition, with regards to further areas that could be covered to achieve convergence of practices in the context of cloud outsourcing, we suggest the following topics be addressed by further recommendations:

- **Security assessment questionnaires:** At present, individual institutions request CSPs complete different assessment questionnaires. It would be beneficial if regulators standardised security assessment questionnaires between institutions and CSPs.

- **Consistency in format of regulations:** The adoption of a standard taxonomy between regulators across jurisdictions would enable institutions to compare and normalise regulatory controls across the jurisdictions in which they operate, driving greater harmonisation of standards.

- **Impacted entities:** These recommendations apply to credit institutions. However, as the financial services landscape evolves, new entrants in the form of financial technology firms (FinTech) may fall outside the scope of covered institutions. Extending the recommendations to other entities, such as FinTech companies, will be important to promote a level playing field within the EU and to ensure risks are being systematically addressed.

The accompanying annex to this letter details our comments in response to the specific recommendations outlined in the consultation.

We would be happy to discuss any of the points raised in more detail.

Yours sincerely,

Daniel Trinder  
Global Head, Regulatory Affairs  
Compliance
ANNEX – Detailed comments on the Recommendations on outsourcing to cloud service providers

4.2 Duty to adequately inform supervisors

- The recommendations suggest that outsourcing institutions should adequately inform competent authorities of material activities being outsourced to cloud service providers and make available certain information, including its risk analysis for the material activities outsourced. It is not clear whether the purpose of this notification to enable regulators to manage concentration risk or to test an outsourcing institution’s risk management. Given the broad definition of “material”, regulators are likely to receive a substantive volume of notifications.

- Greater clarification on the treatment of Non-Material Outsourcing would be helpful for the industry. In particular:
  - Whether competent authorities require an institution to maintain additional information on record of its risk analysis for Non-Material Outsourcing activities (for example, business continuity plans).
  - If an institution can take a risk based approach to Non-Material Outsourcing requirements. For example, not requiring business continuity plans if risk analysis does not deem it necessary.
  - The guidance is unclear on how to address risk analysis for Non-Material Outsourcing as all the regulatory outsourcing requirements apply to both Material and Non-Material Outsourcing, with the exception that Material Outsourcing requires approval/notification of competent authorities. This may result in disproportionate resources spent by institutions on compliance requirements for Non-Material Outsourcing, for example in the case of low value Software as a Service (SaaS) tools that do not host any personal or customer data or Bank confidential information.

4.3 Access and Audit Rights

We refer to the general points raised in our cover letter around audit provision. A different approach to the audit provisions might result in a better outcome in terms of information security. For example, rather than detailing criteria for contract negotiations, the recommendations could suggest CSPs conduct their own audits.

For institutions

- Requesting the right to onsite access of CSPs’ business premises for institution audits is a challenge in negotiations with CSPs who claim that granting unrestricted rights of inspection and auditing to all of their customers generates risks and results in possible disruptions to CSP business. With regards to what is considered an impediment to audit:
  - The suggestions in this section refer to the use of pooled audit information only if the outsourcing institution does not employ its own audit resources. It would be preferable if this would be an acceptable alternative audit right to institutions.
  - A common limitation imposed in contracts for institution audit rights is limiting the number of audit rights per annum. We recommend that the EBA clarify that such limitations are considered an impediment to the rights of access and audit.
  - In practice contracts often limit institution audit rights to ensure that the institution cannot audit subcontractors of the CSP. Some CSPs limit audit rights to sub-processors that process personal data on behalf of the institution only. Further guidance would be helpful for the industry on what would be considered an impediment or limitation, such as specifying what subcontractors competent authorities require the institution to have direct audit rights on.
  - A common limitation imposed in contracts for institution audit rights is the right of the CSP to impose charges on conducting audits. We recommend that the EBA clarify that such limitations are considered an impediment to the rights of access and audit.
• We would welcome clarification that a different risk approach can be taken in relation to audits for Non-Material Outsourcing by institutions and their auditors.

For Competent Authorities

• Requesting the right to onsite access of CSPs’ business premises for competent authority audits is a challenge in negotiations for contracts with CSPs, as CSPs argue that granting unrestricted rights of inspection and auditing to all their customers generates various risks and can cause disruptions to CSP business. We recommend that the EBA suggest alternative measures that would be acceptable to competent authorities similar to the right to pooled audit information for institutions.

• Greater clarity on when competent authorities would need to perform supervisory tasks would be helpful to the industry as most CSPs are unfamiliar with competent authority requirements.

• Many CSPs require third party auditors, including competent authorities, to sign nondisclosure agreements before receiving any audit information. Further guidance on this issue would be helpful for the industry, including on what assurances could be provided to CSPs to address their concern about confidentiality.

• A common limitation imposed in contracts for competent authority audit rights is that the competent authority cannot audit subcontractors of the CSP. Some CSPs limit audit rights to sub-processors that process personal data on behalf of the outsourcing institution only. Further guidance on what would be considered an impediment or limitation on this practice is required, such as on what subcontractors competent authorities would require direct audit rights on.

• In relation to audits for Non-Material Outsourcing by competent authorities, clarity should be provided over whether it is expected that different risk approaches could be undertaken.

4.4 In particular for the right of access

• Providing examples of when a right of access would be required due to an emergency or crisis situation would be helpful for the industry as most CSPs insist on prior notice. This could include whether alternative measures would be acceptable, for example in the case of CSP security escalation processes for security related incidents.

• Further clarity should be given as to whether it is considered an impediment to undertaking audits in the case that a CSP contractually imposes charges on its requirement to cooperate with competent authorities as well as the institution and its auditors for an onsite visit.

4.5 Security of data and systems

• The security guidelines could be more comprehensive, for example in elaborating on information security requirements for CSPs and providing even greater coverage beyond the CEBS guidelines. In particular CEBS guideline 8 (2)(e) references only confidentiality but could be updated to include integrity and availability.

• Section 4.5 (16)(c) would benefit from including access control as an example control area, as it is a particular point of complexity with the secure use of CSPs.

4.6 Location of Data and Data Processing

• Most CSPs require the contractual right to change a data processing location without the institution’s consent. However, moving data location can cause institutions to breach data protection rules and regulations that restrict the offshoring of data. We recommend the EBA provide further guidance on this issue, in particular regarding the provision of notice periods to the institution on a change of location and whether a right to terminate the outsourcing contract would be considered acceptable.
In practice many CSPs argue that they cannot agree to individual notifications and that all clients will be informed centrally, such as through a central portal. We see no reason why a CSP couldn't write separately to each client on such an important issue as change of data location. Accordingly, we would recommend further EBA guidance to this effect.

In addition, given changes in data location can lead to a breach of regulatory requirements on the part of the outsourcing institution, we recommend that the EBA mandate that both regulators and outsourcing institutions have the right to dictate where data moves or should move to, subject to regulatory requirements.

4.7 Chain Outsourcing

The recommendations suggest that the outsourcing agreement between the outsourcing institution and the CSP should specify any types of activities excluded from potential subcontracting. Providing examples of which types of activities institutions should consider for exclusion from potential subcontracting by the CSP would be helpful for the industry.

As per the above, in practice many CSPs argue that they cannot agree to individual notifications and that all clients will be informed centrally, such as through a central portal. We see no reason why a CSP couldn't write separately to each client on the change of subcontractors. Accordingly, we would recommend further EBA guidance to this effect.

Guidance should be provided on the types of subcontractors that should be set out in the contract, for example if it is only those subcontractors performing material or significant activities as part of the outsourced services. This could be based on examples of what competent authorities would consider as significant activities. Many CSPs want to limit notification rights for changing subcontractors to “material” subcontractors or “sub-processors” who process personal data only.

4.8 Contingency Plans and Exit Strategies

There should be clarity ensuring that detailed exit plans may not be necessary for certain Non-Material outsourcing arrangements.

The EBA should clarify what is expected in terms of contingency plans and exit strategies, such as whether it is sufficient for these to be in place internally with the outsourcing institution, or whether they should these be reflected in the commitment within the service provider.