(Submitted via online form)

Dear Sir/Madam,

**Standard Chartered’s response to the European Banking Authority’s (EBA) Consultation Paper on draft Guidelines on Outsourcing (EBA/CP/2018/11)**

Standard Chartered welcomes the publication of the EBA’s revised Guidelines on Outsourcing and the opportunity to provide comments. The update is timely. Since the Committee of European Banking Supervisors (CEBS) published its guidance\(^1\) on outsourcing in 2006, the nature and scale of outsourcing within the financial services sector has grown significantly. This trend is set to continue, as financial technology innovation creates new opportunities, changes competition within the sector, and leads to new third-party dependencies and associated risks. As an international bank, we have seen similar initiatives from global standard setting bodies, as well as regional and national authorities to ensure the regulatory framework for outsourcing is updated and fit for purpose. We encourage the EBA to ensure that these Guidelines are aligned to such efforts and are drafted to accommodate innovation within the industry.

We support the efforts of the EBA to align the requirements applicable to outsourcing arrangements across existing EU regulations and market segments. Ensuring a level playing field is a central role of the European Supervisory Authorities. Consistency in the requirements applicable to credit institutions and payment services institutions (hereafter, institutions) with those of investment firms will provide certainty on the regulatory environment that institutions operate within, enhance competition within the market, and ensure that supervisors can assess the individual and aggregate risks to the broader financial system resulting from outsourcing arrangements.

Broadly, the revised Guidelines set out in the consultation paper are welcome. We recommend, however, that the EBA gives further consideration to the following areas, which we believe to be of material importance:

1. **Treatment of intragroup outsourcing**

   Standard Chartered supports the application of the Guidelines to intragroup arrangements. This is in line with existing regulation and risk management. However, we are concerned that the revised Guidelines do not adequately consider the difference in risk profile between outsourcing intragroup and outsourcing to a third-party service provider. Broadly, applying the same requirements to intragroup outsourcing arrangements may give rise to significant burdens without leading to material improvements in risk mitigation. Our answers to the consultation questions indicate where we believe regulatory relief is appropriate for intragroup arrangements.

2. Proportionate application of the Guidelines and definitions
We welcome the EBA’s approach to ensure proportionate application of the Guidelines, which aims to ensure the risk-sensitive assessment and supervision of outsourcing arrangements. However, we are concerned that the broad definitions of ‘outsourcing’ and ‘sub-outsourcing’ proposed will lead to many arrangements that are not typically considered to be outsourcing arrangements becoming subject to the requirements. While we appreciate that the EBA is seeking to align with the definition set out under the amended Markets in Financial Instruments Directive (MiFID II) framework, there would be practical challenges in implementing the Guidelines based on the current definitions, especially as the definitions are not aligned with other regulatory definitions of outsourcing in place in key centres in which Standard Chartered operates. We have proposed amendments to these definitions in our answer to Question 1. We also recommend that the EBA considers further the level of application for sub-outsourcing arrangements, in particular where sub-service providers do not provide a service that is directly connected to the delivery of an outsourced activity or service, and for the sub-outsourcing of non-critical arrangements.

Further, while we welcome the distinction in the application of some of the requirements between critical and non-critical outsourcing, we are concerned that documentation and risk management requirements may lead to disproportionately high operational and compliance burdens for institutions, as well as potentially divert supervisory attention from those outsourcing arrangements that materially impact the risk profile of an institution.

3. Scope of application
We acknowledge that, in line with EU prudential regulation, the revised Guidelines would apply to all legal entities of an EU parent institution. We recognise the importance of this in the context of ensuring appropriate group-level supervision, but remain concerned over the extraterritorial impact of the requirements, which may lead to implementation obstacles, including legal impediments, when applied to third-country subsidiaries. We provide more detail on this in our answer to Question 1. We also recommend that the EBA considers the competitive impact of applying these Guidelines to entities located in, and outsourcing within, third-country jurisdictions, particularly when contractual rights or the expectations of supervisory authorities differ materially from local market practice. This should be undertaken to avoid duplications or conflicts between the EBA’s requirements and those in third countries, which will cause compliance challenges.

4. Cooperation agreements between supervisory authorities
Existing EU regulation provides for cooperation agreements between supervisory authorities for a limited set of circumstances. The proposed Guidelines seek to extend current arrangements to apply where a banking or payment service is outsourced in full. While we acknowledge that this situation is rare, we are nevertheless concerned with the cliff-edge risk that this presents, as any outsourcing of this nature without a cooperation agreement in place would be prohibited when the Guidelines enter into force. We recommend the EBA considers other existing supervisory arrangements that may facilitate the cross-border supervision of such outsourcing, including supervisory colleges or relevant equivalence determinations, and recognises that cooperation agreements may be informal.

Further, we are concerned that the current drafting implies that cooperation agreements may be required between two third-country supervisory authorities, as the scope of the Guidelines includes all legal entities of EU parent institutions, such as in the case of outsourcing between two third-country subsidiaries of an EU parent institution. We understand that this is not the intention of the EBA and may be an unintended consequence. Accordingly, we would recommend that the EBA confirms that the requirement for cooperation agreements applies only in the case of outsourcing from an EU entity to a third-country entity.

5. Impact on innovation
We note the important role that the EBA is undertaking in developing an appropriate regulatory environment for technology innovation within the sector. We are, however, concerned that some aspects of the proposed Guidelines may inhibit the ability for banks to partner with financial technology firms to develop, and keep pace with, innovative solutions to the industry’s problems and for the benefit of customers. In particular,

---

2 Commission Delegated Regulation (EU) 2017/565, Article 2(3)
excessive constraints around governance and contractual requirements may lead to implementation obstacles at the level of the service provider, and the additional burden may make partnering with EU institutions less competitive. We provide more detail on this concern in our answer to Question 10. The accompanying annex to this letter details our comments in response to the specific questions outlined in the consultation paper.

We hope these comments are helpful, and we would be pleased to discuss our views with you in greater detail.

Yours sincerely,

Ian Sayers
Global Head, Group Regulatory Liaison and Acting Global Head, Regulatory Reform
Compliance
ANNEX – Responses to the questions in the Consultation Paper

Q1: Are the Guidelines regarding the subject matter, scope, including the application of the Guidelines to electronic money institutions and payment institutions, definitions and implementation appropriate and sufficiently clear?

We welcome efforts by the EBA to ensure harmonisation of the requirements applicable to outsourcing arrangements across existing EU regulations and market segments. Ensuring a level playing field is a central role of the European Supervisory Authorities and efforts to ensure consistency across the regulatory framework are important. Further, we support the update to the existing CEBS Guidelines\(^3\) on outsourcing. The nature and scale of outsourcing within the financial services sector has changed significantly since these Guidelines were issued in 2006, and will continue to change to reflect the opportunities that innovation brings, the evolving nature of operational risk and resilience, as well as unforeseen challenges. We encourage the EBA to ensure that these Guidelines are drafted to accommodate such changes and support innovation within the industry.

With respect to the scope of application, we acknowledge that under paragraphs 9 and 17, the proposed Guidelines would apply at group level and across all legal entities structured under an EU parent, where there are no waivers granted under the Capital Requirements Regulation\(^4\) and 4\(^{th}\) Capital Requirements Directive\(^5\). This is wider than the existing MiFID II requirements on outsourcing that the EBA is seeking to align with that, broadly, do not apply to subsidiaries located in third countries. This extends the geographic scope of application to include third-country subsidiaries, including where those entities may be outsourcing services to other entities located in the same or other third-country jurisdictions. While this is overseen at local and group levels, we are concerned that some of the requirements set out in the Guidelines may be difficult to satisfy in cases of outsourcing between two third-country entities.

Further, the extraterritorial application may pose a competitive disadvantage to EU institutions, due to the proposed scope of application across all legal entities, in particular where the proposed Guidelines differ materially to local market practice or standards. Third-country headquartered institutions operating in the same third countries as EU institutions would not have to apply the same level of requirements, as they are not subject to the requirements at a consolidated level. Further impacts arising from the scope of application are highlighted in our answers to following questions.

We are concerned that the definition of ‘outsourcing’ provided in paragraph 11 is too broad, which may in turn result in too broad a definition and identification of critical outsourcing. We understand that the EBA seeks to align with the current definition provided for under MiFID II, but nevertheless believe that the definition would capture broader services provided that are outside of the scope of what is generally considered to be outsourcing. In particular, the definition does not seem in line with paragraph 23 of the Guidelines.

In considering a more appropriate definition, we recommend that the EBA include ‘continuing’, to reflect the fact that outsourcing involves an ongoing arrangement. This would also align the EU definition with the international standards on outsourcing published by the Joint Forum.\(^6\) While this would ensure some alignment with the international definition, we highlight to the EBA that the proposed definition is not in line with that in other major centres in which Standard Chartered operates, in particular with the definitions in Singapore and China. While we understand that the Guidelines would not supersede local regulation, international alignment of clear, simple and pragmatic definitions are key to ensure effective implementation.

---


\(^4\) Under Articles 7 and 10 of Regulation (EU) 575/2013

\(^5\) Under Article 21 of Directive 2013/36/EU

\(^6\) [www.bis.org/publ/joint12.pdf](https://www.bis.org/publ/joint12.pdf), Section 3
Similarly, we are concerned that the definition of ‘sub-outsourcing’ is too broad. We are aware that the level of sub-outsourcing has been the subject of debate among European regulators, in particular with regards to the EBA’s December 2017 Recommendations on Outsourcing to Cloud Service Providers\(^7\). Nevertheless, we recommend that the EBA adjusts this definition to apply to sub-outsourcing where ‘a fourth-party provides in part or full a process, service or activity which is directly connected to the provision of the outsourced service classified as an outsourcing arrangement with a third-party.’ Without adjustment, the current definition may place an undue regulatory burden on the outsourcing institution if the sub-outsourced activity is not material to the delivery of the outsourced service or activity. We would support further efforts by the EBA to focus on the sub-outsourcing of critical outsourcing arrangements, to ensure the Guidelines are implemented in a risk-based and proportionate way. We are concerned, for example, that the current definition would include legal and HR firms, which should be excluded from scope as they are for outsourcing under paragraph 23 of the proposed Guidelines. In considering its treatment of sub-outsourcing, we recommend that the EBA considers the practical implementation challenges that firms will face in monitoring all aspects of these arrangements.

We are grateful that the EBA proposes to phase-in the application of the Guidelines with respect to arrangements that were entered into before the indicative date. This reduces the operational burden on institutions and the potential commercial impact of renegotiating arrangements that may have been in place for some time to include new provisions. For new arrangements, however, we note that the indicative date may follow final publication by a matter of months. For example, the EBA consultation on Recommendations for Outsourcing to Cloud Service Providers closed in August 2017 and final Recommendations were published in December 2017. Following this indicative timeline for these Guidelines, institutions may only have 3-5 months to implement potentially significant operational and systems changes as the Guidelines apply in full to all new arrangements and across all legal entities after this date. To remedy this, we recommend that the EBA provides institutions and national competent authorities at least 12 months to implement the Guidelines. In line with our answer to Question 3, we also request that the EBA considers which pre-existing supervisory arrangements may already be in place to avoid a cliff-edge in the implementation of the requirement for cooperation agreements with third-country supervisory authorities, such as supervisory colleges.

Finally, we welcome that the EBA provides transitional provisions in paragraph 13 that allow institutions until 31 December 2020 to complete the documentation requirements under Section 8.

Q2: Are the Guidelines regarding Title I appropriate and sufficiently clear?

We welcome the EBA’s proportionate approach to compliance and monitoring. Proportionality is a central principle of EU regulation and ensures appropriate focus and risk-based supervision. We believe that the principle of proportionality can also apply to the nature of outsourcing agreements. We welcome that the consultation paper differentiates between critical and non-critical outsourcing, but some of the requirements may lead to excessive compliance or operational burdens, as well as compromise effective and risk-sensitive supervision. In that sense, we recommend that the EBA: adjusts the definitions of outsourcing and sub-outsourcing in line with our answer to Question 1; restricts the de facto designation of critical outsourcing in line with our answer to Question 7; and gives further consideration to its approach to sub-outsourcing in line with our answers to Questions 1 and 10.

We support the application of the Guidelines to intragroup arrangements, set out in Title 1. This clarifies and strengthens existing EU guidance on outsourcing, and aligns to regulatory frameworks in other jurisdictions. We are concerned, however, that there is little recognition in the draft Guidelines given to the difference in risk profile between intragroup arrangements and outsourcing to third-party service providers,

\(^7\)https://www.eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8b2f1e
as the Guidelines apply to all outsourcing arrangements. We were encouraged by the feedback provided by the EBA at its Open Hearing on 4 September that the regulatory treatment of intragroup outsourcing should be different, and support efforts to further consider such differences when drafting the final Guidelines that will apply to intragroup arrangements. Applying requirements designed for third-party outsourcing to intragroup arrangements may lead to operational inefficiencies and an approach that does not apply risk-based principles.

For example, we believe it is unnecessary to require an exit strategy for intragroup arrangements. An intragroup arrangement would not be exited in the same way that an institution would exit an arrangement with a third-party. Business continuity plans for such intragroup arrangements, as well as operational resilience measures that ensure short-term recovery from operational incidents, already deal adequately with the failure of a supplier. We provide more detail on this in our answer to Question 12.

Another and more significant example is in relation to paragraph 26, which requires cooperation agreements to be agreed by supervisory authorities to allow for the outsourcing of banking activities or payment services to third countries. As noted in our answer to Question 1, such cooperation agreements may not be needed for intragroup arrangements under a risk-based approach. Home supervisory authorities have access to other group entities for the purposes of consolidated supervision, including non-banking entities, and existing arrangements to facilitate this supervision are likely to be already in place.

Q3: Are the Guidelines in Title II and, in particular, the safeguards ensuring that competent authorities are able to effectively supervise activities and services of institutions and payment institutions that require authorisation or registration (i.e. the activities listed in Annex I of Directive 2013/36/EU and the payment services listed in Annex I of Directive (EU) 2366/2015) appropriate and sufficiently clear or should additional safeguards be introduced?

Generally, the Guidelines in Title II are sufficiently clear. We recommend that the EBA amends paragraph 22 to include intragroup arrangements as well as arrangements with third-party service providers to ensure consistency with Title I of the Guidelines, and to provide clarity to institutions and supervisory authorities that the Guidelines apply to intragroup arrangements.

In line with our answer to Question 1, we support the clarification that the EBA provides in paragraph 23 that the acquisition of services, goods or utilities not normally performed by institutions is not to be considered as outsourcing, and recommend that the EBA maintains this as a non-exhaustive list. While Standard Chartered subjects all arrangements with third parties to a risk-assessment, we believe that paragraph 24 extends beyond the objective of the Guidelines and the principle of proportionality.

Further, we would support additional clarity from the EBA that the acquisition of services, goods or utilities that themselves depend on cloud technology, at the level of the third-party supplier, is not automatically defined as ‘cloud outsourcing’ for the purposes of the purchasing entity. We do not believe this is the expectation of the EBA, but want to avoid this potential unintended consequence.

Regarding paragraph 26 and the requirement that cooperation agreements are put in place with third-country supervisors, we are grateful for the clarification that the EBA provided at its Open Hearing on 4 September that such agreements will only need to be in place for the outsourcing in full of a banking or payment service, such as those listed in Annex 1 to the 4th Capital Requirements Directive. In accordance, we recommend that in the final Guidelines the EBA clarifies the language to make this clear, and considers direct reference to banking and payments services defined in EU legislation, and as referred to in the question. In line with our answer to Question 2, we would also encourage the EBA to mitigate the cliff-edge impact of this requirement by considering existing supervisory arrangements that ensure an appropriate level of oversight.
Further, we are concerned that an unintended consequence of the current drafting is that a cooperation agreement may be required between two third-country supervisory authorities where a banking service is outsourced between two third-country subsidiaries of an EU parent institution. We welcome the clarity that the EBA provided at its Open Hearing on 4 September that this is not the intention and that these Guidelines cannot bring about this requirement. Nevertheless, we remain concerned as the proposed Guidelines apply to every legal entity of an EU parent institution. Accordingly, we would welcome an amendment to paragraph 26 to make clear that the requirement for a cooperation agreement applies only to outsourcing arrangements from an EU entity to an entity located in a third-country.

Without clarification on these two points, paragraph 26 may represent a significant inhibiting factor to the ability of EU institutions to outsource to third countries. We recommend the EBA in its final Guidelines considers the competitiveness of EU-headquartered institutions and, in line with our answer to Question 2, applies regulatory relief from this requirement where the service provider is part of the same group.

Finally, with respect to the requirement in paragraphs 25 and 26 that the service provider is authorised in that member state or third-country jurisdiction to perform the outsourced banking activity or payment service, we highlight that there is not an internationally consistent approach to regulated activities. While this requirement is broadly consistent with the CEBS guidance, it differs in that it applies to a broader set of financial services, including payment services. We recommend that the EBA considers this in the final Guidelines.

Q4: Are the Guidelines in Section 4 regarding the outsourcing policy appropriate and sufficiently clear?

We believe that the Guidelines in Section 4 are appropriate and sufficiently clear.

Q5: Are the Guidelines in Sections 5-7 of Title III appropriate and sufficiently clear?

Generally, we agree that the Guidelines in Sections 5-7 are appropriate and sufficiently clear. However, we recommend that the EBA gives further consideration and guidance on the types of tests that may be appropriate for different outsourcing arrangements, taking into account the differing risk profiles of the outsourced arrangements. For example, and in line with our answer to Question 2, desktop walkthroughs may be sufficient in the case of intragroup outsourcing where an outage will result in a transfer to other existing internal systems or teams. Testing involving full service outage simulation and recovery are generally more appropriate for business continuity planning in the case of a critical outsourcing arrangement to a third-party supplier. Furthermore, while business continuity plans should be tested, there is limited value in requiring joint exercises with third-party suppliers, as business continuity plans assume the failure of that supplier. There are some circumstances where testing may be appropriate, such as partial failures and where the service provider is co-located with the outsourcing institution, and we encourage the EBA to consider these nuances when drafting its final Guidelines.

Please see our answer to Question 10 for our concerns on ensuring unrestricted rights to information and audit, referencing Section 10.3.

As mentioned in our cover letter, continuing innovation across the sector will lead to shifts in the provision of financial services to clients and consumers. It is important that these Guidelines also account for the scenario where institutions are playing the role of a service provider in the provision of financial services, outsourced from both the regulated and non-regulated sectors. Accordingly, requirements for unrestricted rights of access to systems, premises and data may lead to information security, competition and commercial concerns.
Q6: Are the Guidelines in Section 8 regarding the documentation requirements appropriate and sufficiently clear?

We welcome the requirement to maintain a central register of all outsourcing arrangements. This will facilitate effective internal controls, oversight and risk management within institutions, and will aid the effective supervision of such arrangements. As noted in our answer to Question 1, we also welcome the EBA’s proposed transitional timeline for implementation of the register, which recognises that institutions may need to make amendments or enhancements to existing systems to comply with the criteria set out in Section 8.

We do, however, believe that certain amendments are needed to ensure that the requirements can be implemented in a practical manner, which avoids undue burdens or disruption to arrangements that are currently in place. In the case of intragroup outsourcing, there is duplication between the requirement to record all outsourcing arrangements at legal entity level (paragraph 46) and the requirement that all entities within the scope of prudential consolidation that make use of the outsourcing are listed (paragraph 47(a)(v)). In such cases, it should be sufficient to list the legal entities within the prudential scope of consolidation that make use of the intragroup arrangement, without also needing to record separate entries for each legal entity.

With respect to the requirements to record information on sub-service providers set out in paragraph 47(b), we recommend that the EBA provides guidance on the level of sub-outsourcing required. As noted in our answer to Question 1, as well as in our feedback to the EBA’s consultation on Recommendations for Outsourcing to Cloud Service Providers, we recommend that the EBA restricts the requirements on sub-outsourcing to those arrangements that are directly connected to the provision of the service and the sub-outsourcing of critical outsourcing arrangements.

With respect to cloud service providers more generally, we remain concerned that it can be difficult for an institution to meet all requirements proposed by the EBA, including to obtain the proposed level of information on sub-service providers. To ensure effective implementation, we recommend that proportionality is applied. Institutions should be allowed to assess the criticality of data stored on the cloud and be given the flexibility to determine appropriate governance and risk management procedures for cloud outsourcing that is non-critical. As regulators from various jurisdictions have differing requirements with respect to cloud technology, such flexibility would allow institutions with a global footprint to adopt an appropriate cloud strategy that is aligned to applicable data protection rules. Such flexibility would encourage the adoption of cloud technology and would ensure that EU institutions remain competitive in this global market.

Q7: Are the Guidelines in Sections 9.1 regarding the assessment of criticality or importance of functions appropriate and sufficiently clear?

We support the conditions set out by the EBA in paragraph 49 for those arrangements that should always be considered as critical outsourcing. We recommend, however, that the EBA provides further guidance on whether all operational tasks of internal control functions should be automatically designated as critical outsourcing. While not detracting from the internal control function itself, or indeed from the fact that institutions cannot outsource their regulatory obligations or accountability for compliance with regulatory obligations, it is possible that operational tasks related to control functions can be non-critical.

More significantly, we are concerned that the wording in paragraph 50 is too broad, in that it defines any activity, process or service ‘relating to’ core business lines as critical outsourcing. Given the potentially very

---

broad implications of the term ‘relating to’, we believe that such a requirement may give rise to many non-critical arrangements being automatically defined as critical outsourcing arrangements. This is disproportionate and would risk diverting internal risk management and supervisory attention towards activities or processes with a materially lower risk profile. Moreover, the existing wording does not take into account the volume of the service or function that is outsourced. For example, a small volume of a critical service might be outsourced to a third-party, with the majority remaining internal. Accordingly, we recommend that the EBA aligns the wording of this paragraph with that of paragraph 51; that activities, processes or services ‘directly connected with the provision of’ core business lines and critical functions should always be considered as critical outsourcing. Such wording would allow institutions the flexibility to take a risk-based view on whether wider arrangements should be considered critical, in line with Section 9.3. On paragraph 51, we support the EBA’s view that this list is not exhaustive and that thresholds should not be put in place that give rise to an automatic classification as critical.

In line with our answer to Question 2 on differentiating intragroup outsourcing, some of the criteria for the assessment of criticality may lead to incorrect assessments in the case of intragroup arrangements. These include the criteria for assessing the substitutability and/or the ability to reintegrate an outsourced function. In the case of intragroup outsourcing to a group service centre, for example, it is unlikely that the outsourced service would need to be substituted or reintegrated. More generally, we are concerned by the number of criteria set out across paragraphs 49, 50 and 51. While we appreciate the EBA’s efforts to provide granular requirements, this may lead to an overly restrictive outcome as well as requirements that are difficult to interpret and implement. Accordingly, we recommend the EBA considers whether these criteria can be simplified and streamlined, to avoid unnecessary complexity. In doing so, we encourage the EBA to align as far as possible with regulatory frameworks in other jurisdictions, which would facilitate effective implementation for EU institutions.

Q8: Are the Guidelines in Section 9.2 regarding the due diligence process appropriate and sufficiently clear?

In line with our answer to Question 2, some of the criteria to conduct due diligence would not be necessary for intragroup outsourcing. This includes requirements to consider the service provider’s business model, nature, scale, complexity and financial situation. These assessments would be redundant and, in some cases, will be dependent on the outsourcing arrangement itself.

We welcome the EBA’s guidance that institutions should take appropriate steps to ensure that service providers and sub-service providers act in a manner consistent with the outsourcing institution’s values and code of conduct, as well as adhere to international standards on human rights, environmental protection and the prohibition of child labour. Standard Chartered’s brand promise is to be Here for Good, which extends to the third parties that we do business with. Institutions and supervisory authorities can and should work together to ensure these international standards are adhered to wherever and whenever they operate.

Q9: Are the Guidelines in Section 9.3 regarding the risk assessment appropriate and sufficiently clear?

In line with our answer to Question 3, while we conduct risk assessments for all third-party suppliers, we are concerned that the EBA proposes the same level of prescription for all arrangements with third parties, even those that are not considered to be outsourcing arrangements. An extension of the scope of the document to arrangements beyond those defined as outsourcing is not in line with the principle of proportionality, which itself is set out within the consultation paper.
We agree with the EBA that institutions should assess the impact of the outsourcing arrangements on their operational risk profile, as well as take appropriate steps to avoid undue additional operational risks arising from such outsourcing arrangements. However, the requirement to conduct risk assessments based on ‘scenarios of possible risk events’, as set out in paragraph 58, is overly burdensome. Risk assessments, by their nature, consider the high-level impacts of failed or inadequate services received, rendering a full scenario-based stress-test of the arrangement unnecessary. Further, we note that despite references to the principle of proportionality, this requirement applies to all outsourcing arrangements. While we agree that there are certain risks that need to be assessed across all arrangements, applying a scenario-based analysis of all possible risk events across all outsourcing arrangements would create an administrative, operational and compliance burden. If this requirement is maintained, we recommend that such scenario-based assessments and related documentation of the test performed, test results and conclusion as to whether the arrangement would increase or decrease an institution’s operational risk should be limited to critical outsourcing arrangements.

Further, we note here work among regulatory bodies both at the international level and within the UK on ensuring operational resilience. Without detracting from the policy objective of assessing the risk of outsourcing arrangements, we recommend that the EBA ensures that its outsourcing Guidelines are aligned to these policy initiatives. In particular, requirements to conduct scenario-based analysis on each agreement may create an additional burden if future regulatory initiatives on operational resilience also focus on impact assessment and planning at the level of business services.

Finally, we note that paragraph 61(d) requires the assessment of political stability and the security situation of the jurisdiction of the service provider. This concept is also mentioned in paragraph 41 on business continuity planning. While we understand why the EBA may wish to include this, we are concerned that too heavy a weighting to this risk factor may lead to divergent views among institutions and their supervisors. Additionally, there may be important political, economic or social factors that institutions may need to consider before taking a decision to alter or withdraw from an outsourcing arrangement, notwithstanding the risk identified.

Q10: Are the Guidelines in Section 10 regarding the contractual phase appropriate and sufficiently clear; do the proposals relating to the exercise of access and audit rights give rise to any potential significant legal or practical challenges for institutions and payment institutions?

We believe that the proposals relating to the exercise of access and audit rights, such as the requirement to include ‘unrestricted’ and ‘complete’ rights of access within the outsourcing agreement, give rise to significant implementation challenges for institutions. Paragraphs 63(h), 72(a) and 72(b) of the proposed Guidelines contain this requirement. There are many legitimate reasons why service providers may not agree to contractual terms and the exercise of complete access to the full range of devices, systems, networks, information and data used for providing the outsourced service, and only agree to those relevant to the delivery of the service, as well as requiring a reason or prior notice. These reasons include security requirements, the risk of service disruption, data privacy, the protection of client data and other processes related to clients, as well as various commercial and competitive factors.

As a result, we recommend that the EBA limits both access and audit rights to what is necessary to monitor the outsourcing requirement, adequately assess and control any arising risks, and comply with all applicable regulatory requirements. It should also be noted that depending on the nature of the service provider, it may not be relevant to ensure direct access to a physical centre. This is the case, for example, with cloud service providers. Instead, it would be more appropriate to ensure that cloud service providers can demonstrate that their processes are properly performing their roles, which may not be able to be assessed via on onsite visit. It should also be noted that adding these rights to an established relationship when renewing existing arrangements in order to comply with the proposed Guidelines may be difficult, or may have a significant commercial impact on the outsourcing institution.
Further, we are concerned that the proposed Guidelines and the mandatory right to audit may impede the financial technology and innovation ecosystem, inhibiting the competitiveness of EU firms. For example, the ability for a bank to partner with a small third-party vendor on the development of an innovative product or service may be impeded if that third-party provider could not secure the contractual right to audit a large cloud service provider, in the case that it was hosting in the cloud, which would become a prerequisite of the initial outsourcing under the proposed Guidelines. While we agree that institutions should manage the risks they are exposed to, the requirement does not seem to be proportionate. In this example, it may prevent the deployment of the innovative solution as the vendor is not subject to the regulatory requirement and so has no right to ensure audit rights to the cloud service provider. We recommend the EBA considers an approach that allows institutions to take a proportionate approach, based on an understanding of the scale of the outsourcing, the exit strategy of the vendor themselves to avoid concentration risk, and the use of audited third-party reports for offsite assessments. We recommend the EBA further considers how to address this point in a manner consistent with its role in supporting innovation within the European banking sector.

We welcome the EBA’s guidance on the use of third-party reports and pooled audits to decrease the operational burden on both institutions and service providers, and provide for an effective solution to where many institutions need to satisfy the same requirement with respect to the same service provider. We recommend the EBA also considers whether this should be extended to cover regulatory inspection reports issued by third-country supervisors. While we acknowledge that the use of such third-party reports and pooled audits cannot replace the governance, risk assessment and control environment that an institution has in place around its outsourcing arrangements, we are concerned that the guidance that such third-party reports and pooled audits cannot be ‘solely’ relied upon may undermine the take-up of such initiatives.

Further, paragraph 75(e) requires a contractual right to request that an expansion of scope of the audit report. In practice, negotiating this condition might be difficult and may not be achievable in all cases, depending on the structure of the pooled audit and the organisation conducting it. Should an institution determine that it would need an expanded scope to satisfy its requirements, it should be able to conduct such an audit individually without undermining the utility of the pooled audit. We recommend that the EBA reconsiders this condition, in conjunction with the above concern that not relying on such pooled audits may limit their practical use.

We also recommend that the EBA provides further guidance with respect to the use of third-party reports to satisfy the requirement for security penetration testing to assess the effectiveness of cyber and internal ICT security measures and processes. As written, the Guidelines imply that institutions are required to carry out the penetration testing themselves. Clarity would be welcome as to whether an independent third-party can be used to perform and report upon such penetration tests. This would be particularly welcome given the expertise and resources that reside within such third parties.

With regards to the sub-outsourcing in Section 10.1, we agree that the requirements should apply to the sub-outsourcing of critical or important functions and, in line with our answer to Question 1, recommend that the EBA limits the application of these requirements to the sub-outsourcing of services directly connected to the provision of the outsourced service, and specifically where a material or significant part of the outsourced service is delivered by a sub-service provider. This is particularly relevant to the conditions set out in paragraph 65, including the obligation to inform the outsourcing institution of planned sub-outsourcing, which as drafted would apply to all levels of sub-outsourcing, and to secure the right to terminate the agreement in the case of undue sub-outsourcing.

We also note a similar concern to that raised above on access and audit rights arising from paragraph 66. In our view, it will become impractical to secure such rights along a chain of sub-service providers and especially where sub-service providers are not conducting a service that is material to the delivery of the service.
With respect to termination rights, introducing the right to allow an institution to terminate the arrangement in the case of ‘weaknesses’ in the management and security of confidential data may be difficult to achieve. The termination of a contract needs to be linked to a breach, or a reduction in service level that constitutes a breach, in particular to avoid legal disputes. While the security of confidential, personal and otherwise sensitive data is a key priority for institutions and service providers alike, it is more appropriate for the right to terminate to be based on a breach of contractual obligations. This is in line with other criteria set out in paragraph 81, which focus on ‘breaches’ of law and ‘identified’ impediments.

Q11: Are the Guidelines in Section 11 regarding the oversight on outsourcing arrangements appropriate and sufficiently clear?

Generally, we believe that the Guidelines in Section 11 are appropriate and sufficiently clear. We welcome the EBA’s intention to limit the reassessment to critical outsourcing, as application to non-critical outsourcing would not be proportionate to the risk and would create an administrative and operational burden. We would, however, welcome more guidance on how often institutions should update their risk assessment under Section 9.3 with respect to outsourcing of critical functions. The frequency of such reassessments should be dependent on the classification of the criticality. Accordingly, we recommend an annual reassessment for all critical outsourcing arrangements. The EBA should consider this issue in conjunction with our answer to Question 9, where we note our concerns about the overly prescriptive and disproportionate requirement to conduct scenario-based analysis covering all risk-types for all outsourcing and non-outsourcing arrangements with third parties.

Q12: Are the Guidelines in Section 12 regarding exit strategies appropriate and sufficiently clear?

Generally, we believe that the Guidelines in Section 12 are appropriate and sufficiently clear. In line with our answer to Question 2, however, we believe that exit strategies are not necessary for intragroup outsourcing arrangements. Business continuity plans, under Section 6 of the proposed Guidelines, address the scenario where the service provider has failed or delivery of the outsourced service is compromised, and establish the necessary conditions to ensure continuity in such an event. This is complemented by measures to increase operational resilience, which ensure the short-term recovery from an operational shock. Exits from intragroup arrangements are fundamentally different to exits from third-party arrangements where it is necessary to bring the service back within the institution. Adjustments to intragroup arrangements should continue to be managed by the institution as part of its business and strategic planning, and should not require formal exit arrangements to be put in place.

In terms of its application to third-party service providers, we recommend that the EBA amends paragraph 90(b) to include ‘access to data’ in the list of what must be removed or transferred from the service provider to alternative providers or back to the institution. With respect to data, we note a further challenge related to the requirement to test data transfers. The transfer of such data should be an important part of setting an exit strategy, but it is not feasible to test the transfer of that data. We recommend removing this requirement.
Q13: Are the Guidelines in Section 13 appropriate and sufficiently clear, in particular, are there any ways of limiting the information in the register which institutions and payment institutions are required to provide to competent authorities to make it more proportionate and, relevant? With a view to bring sufficient proportionality, the EBA will consider the supervisory relevance and value of a register covering all outsourcing arrangements within each SREP cycle or at least every 3 years in regard of the operational and administrative burden.

We support the reporting of outsourcing arrangements to supervisors, in line with paragraph 92. However, we are concerned that given the significant volume of non-critical outsourcing undertaken by institutions, effective and risk-sensitive supervision may be put at risk by the sheer volume of data reported. This is exacerbated by the broad definition of outsourcing, which we have raised in our answer to Question 1, and the lack of a de minimis threshold for outsourcing arrangements to be recorded in the register. Accordingly, to ensure that proportionate and relevant information is provided to supervisors, we recommend that the EBA applies the requirement to critical outsourcing arrangements only. Supervisors should, however, retain the right to request further information on non-critical outsourcing, such as if they become concerned about an institution’s level of operational risk, concentration risk in a particular entity, or its aggregate level of risk arising from the amount of outsourcing that is taking place.

We welcome the EBA’s view on the ex-ante notification of planned critical outsourcing, which is in line with supervisory practice. In particular, harmonisation across the EU is necessary given the different approaches taken by national supervisors. It is commendable that the EBA has not chosen to impose ex-ante assessment and approval by supervisors, as was considered as a policy option in the impact assessment. Such ex-ante approval processes can lead to additional costs for outsourcing institutions, uncertainty over whether and when to engage with service suppliers, and commercial impacts through delays in the implementation of such arrangements.

While ex-ante notification is welcome, it may not be possible in all cases for institutions to provide all information under points (a), (b) and (c) of paragraph 47. Paragraph 47 applies to existing outsourcing arrangements that are recorded in the register, whereas the ex-ante notification requirement applies to planned outsourcing arrangements before they are entered into. Accordingly, not all the information may be available or negotiated when the ex-ante notification is provided. In its consideration of how to make Section 13 proportionate and relevant, we recommend that the EBA works with national supervisors to focus on the information needed for the purposes of effective and efficient supervision, which may come from any of the sections in paragraph 47, but is unlikely to extend to the full set of information proposed.

Q14: Are the Guidelines for competent authorities in Title V appropriate and sufficiently clear?

In general, we believe that the Guidelines in Title V are appropriate and sufficiently clear. We are concerned, however, that there is a lack of clarity for institutions with respect to the monitoring of concentration risk at the sectoral level under paragraph 104, particularly when considered in conjunction with the power for supervisory authorities to limit, restrict or require exit from outsourcing arrangements under paragraph 105. This represents a level of business risk that institutions cannot manage, in particular as individual institutions cannot be expected to know the level of concentration risk at the sector-level.

Moreover, limiting the ability of institutions to undertake outsourcing based on sectoral concentration risk is likely to have commercial implications and a distortive impact on competition. Accordingly, we would welcome clarification by the EBA that national supervisors should monitor and address the build-up of concentration risk at the institution and sectoral level in conjunction with the industry including sufficient open dialogue. At the least, advance notice of the use of supervisory tools to address concentration risk will be necessary to limit any subsequent disruption.
Q15: Is the template in Annex I appropriate and sufficiently clear?

We believe that the template in Annex I is appropriate and sufficiently clear. We welcome the clarification that the EBA provided in its Open Hearing on 4 September that the Annex is intended to be an example template, and that institutions could submit data in other formats providing they are uniform, accessible and cover the required fields. Maintaining this is necessary as institutions already have systems in place for recording information on outsourcing agreements. Institutions should continue to be allowed to use these systems to monitor and report on their outsourcing arrangements, notwithstanding the need to make necessary changes or enhancements to fulfil the requirements set out in these Guidelines.

Q16: Are the findings and conclusions of the impact assessments appropriate and correct; where you would see additional burden, in particular financial costs, please provide a description of the burden and to the extent possible an estimate of the cost to implement the Guidelines, differentiating one-off and ongoing costs and the cost drivers (e.g. human resources, IT, administrative costs, etc.)?

We have indicated the additional burdens arising from these Guidelines in our answers to the above questions.