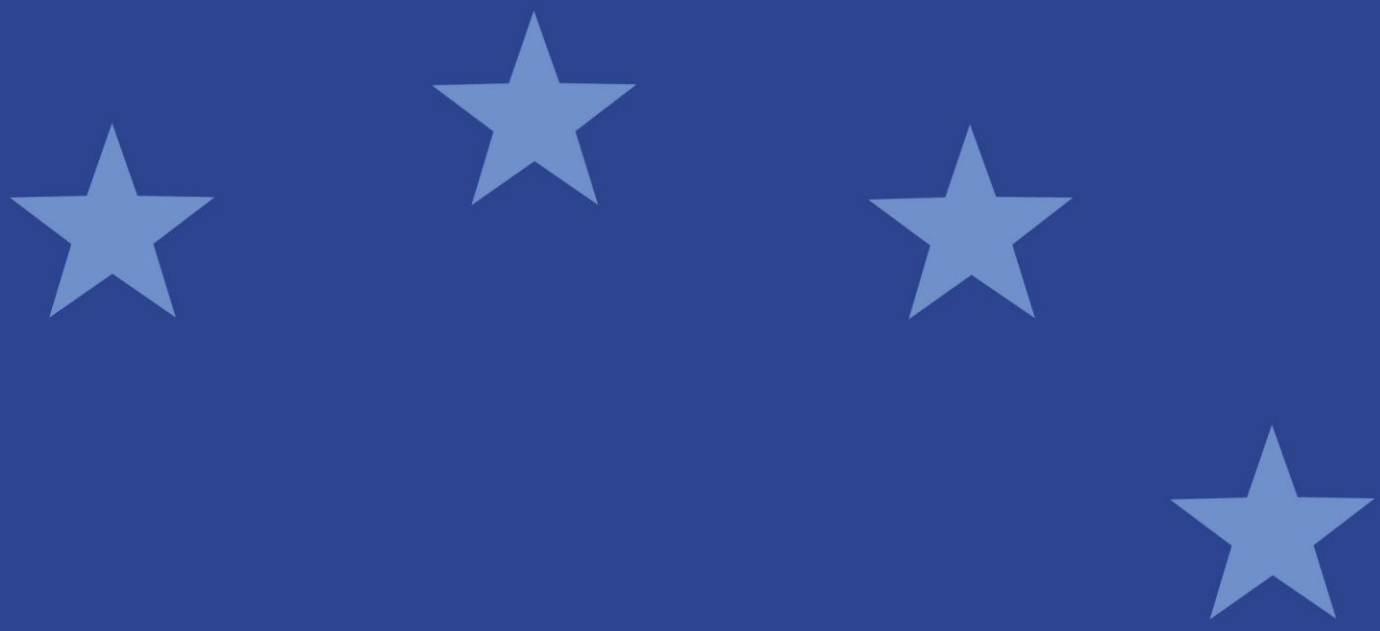
esma European Securities and Markets Authority

Response Form to the Consultation Paper

Guidelines on Outsourcing to Cloud Service Providers



03 June 2020 ESMA-XX-XXX

Responding to this paper

ESMA invites comments on all matters in this consultation paper on guidelines on outsourcing to cloud service providers and in particular on the specific questions summarised in Appendix I. Comments are most helpful if they:

- respond to the question stated;
- indicate the specific question to which the comment relates;
- contain a clear rationale; and
- describe any alternatives ESMA should consider.

ESMA will consider all comments received by **01 September 2020.**

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'.

Instructions

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.

2. Please do not remove tags of the type <ESMA_QUESTION_COGL_1>. Your response to each question has to be framed by the two tags corresponding to the question.

3. If you do not wish to respond to a given question, please do not delete it but simply leave the text "TYPE YOUR TEXT HERE" between the tags.

4. When you have drafted your response, name your response form according to the following convention: ESMA_COGL_nameofrespondent_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA_COGL_ABCD_RESPONSEFORM.

5. Upload the form containing your responses, in Word format, to ESMA's website (www.esma.europa.eu under the heading "Your input – Open consultations" → "Consultation on Outsourcing to Cloud Service Providers").

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA's Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading Legal Notice.

Who should read this paper

This paper is primarily of interest to national competent authorities and financial market participants. In particular, this paper is of interest to alternative investment fund managers, depositaries of alternative investment funds, undertakings for collective investment in transferable securities (UCITS) management companies, depositaries of UCITS, central counterparties, trade repositories, investment firms and credit institutions which carry out investment services and activities, data reporting services providers, market operators of trading venues, central securities depositories, credit rating agencies, securitisation repositories and administrators of benchmarks ("firms"), which use cloud services provided by third parties. This paper is also important for cloud service providers, because the draft guidelines seek to ensure that the risks that may arise for firms from the use of cloud services are properly addressed.

General information about respondent

Name of the company / organisation	Association for Financial Markets in Europe (AFME)
Activity	Investment Services
Are you representing an association?	☒
Country/Region	Europe

Introduction

Please make your introductory comments below, if any

<ESMA_COMMENT_COGL_1>

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on **the ESMA GUIDELINES ON OUTSOURCING TO CLOUD SERVICE PROVIDERS**. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Executive Summary

AFME welcomes the opportunity to support ESMA on the draft guidelines on outsourcing to cloud service providers (CSPs), following the 2018 European Commission Fintech Action Plan[1], and recent guidelines such as the EBA 2019 Guidelines on Outsourcing Arrangements (EBA Guidelines).[2]

As detailed in AFME's 2019 paper '*The Adoption of Public Cloud Computing in Capital Markets'*, cloud computing offers an adaptable and versatile way to consume a range of information technology services, such as business applications, data storage and processing power. It brings a range of benefits, including greater business agility and innovation, improved overall cost management, increased operational efficiency, enhanced client experience and service offerings, and efficient risk management.[3] The COVID-19 pandemic has further

[1] https://ec.europa.eu/info/publications/180308-action-plan-fintech_en
[2] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements
[3] https://www.afme.eu/reports/publications/detail/The-Adoption-of-Public-Cloud-Computing-in-Capital-Markets

emphasized the continued importance of technology, such as cloud services, in enabling resilient and efficient financial markets (e.g. enabling remote access and collaboration). It is important that the benefits of cloud computing are balanced against the potential risks and that adoption is encouraged across the industry in a risk-based approach.

Overall, AFME is in broad agreement on the ESMA draft guidelines, providing a risk-based approach, whilst promoting flexibility to support increased future cloud adoption. However, we would like to raise the following high-level considerations from our response:

- **Alignment with EBA**: We welcome that these guidelines are broadly aligned to the recent EBA Guidelines, however, for firms that will be subject to both, we strongly encourage ESMA to ensure that specific definitions and requirements are in full in alignment with those of the EBA. This will reduce regulatory fragmentation, the compliance burden on firms, and provide greater consistency between supervisory authorities. We have highlighted in our response those areas in which there are currently differences. If this cannot be achieved, then we request confirmation that (for entities in scope of both EBA and ESMA requirements) compliance with the EBA Guidelines would be seen as substituted compliance. However, we note that this approach is not ideal as it leaves open the possibility than individual national competent authorities might create their own requirements based on elements of each set of Guidelines, which would further increase implementation complexity for firms.
- Further, we would welcome any commentary from ESMA on the alignment of the Guidelines to any future measures from the European Commission or the European Supervisory Authorities that may be introduced, such as direct supervisory oversight of third-party providers, such as CSPs.
- **Proportionality**: We support ESMA's references to the principle of proportionality in drafting these guidelines. The range of cloud outsourcing services used within the industry is very broad, which should be reflected in the drafting and application of these guidelines. Firms should be able to take into consideration the size and level of risk of each arrangement (including whether the function is critical/important), as well as whether the arrangement is external or intragroup.

  For example, regarding intragroup outsourcing, the Guidelines should recognise that institutions will have a higher level of control over the outsourced function when outsourcing within the same group (for example, when outsourcing a function to head office). This should be taken into account in their risk assessment, as well as when applying these requirements.

We would also welcome a sufficient period for implementation of the Guidelines once published, such as the suggestion given of December 2022. This will provide firms with an appropriate period to consider any necessary changes and take account of other parallel regulatory activities, such as the development of cloud registers. We note in particular that changes to legacy arrangements are more time consuming than ensuring that new arrangements will be compliant, and that the implementation time will also be directly impacted by how closely ESMA aligns its Guidelines to the existing EBA requirements referenced above.<ESMA_COMMENT_COGL_1>

Questions

Q1 : Do you agree with the suggested approach regarding a firm's governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

<ESMA_QUESTION_COGL_1>
AFME would like to raise the following points:

In relation to paragraph 26c, while we agree that the "nature, scale and complexity" of a business should be considered, we suggest that the role of a firm in the financial system may be a more important factor in assessing risk and assigning responsibility.

<ESMA_QUESTION_COGL_1>

Q2 : Do you agree with the suggested documentation requirements? Please explain.

<ESMA_QUESTION_COGL_2>
AFME would like to raise the following:

Paragraph 28 states that firms must provide a brief summary of the reasons why the outsourced function is or is not considered critical or important. The number of foreseen non-critical functions is high and therefore explaining why each is non-critical would result in a high degree of work which undermines the principle of proportionality and a risk-based approach. We would suggest instead that a firm should have to clarify its criteria and process for determining materiality once, allowing a regulator to request further information in the event that a specific function requires further detail. This would also be better aligned with the EBA Guidelines, which state in paragraph 54 that an explanation is required for why an outsourced function is considered critical or important, rather than why it is not.

In relation to paragraph 29:

(e): *'whether the outsourced critical or important function supports business operations that are time-critical'*. We note that there are multiple ways in which firms may express or record whether an operation is time-critical and request that ESMA allows firms the flexibility to do so according to their internal processes.

(f) requests the brand name and country of registration of the CSP, which goes beyond the corresponding requirement in EBA Guidelines paragraph 54(e(g): *"the governing law of the cloud outsourcing arrangement and, if any, the choice of jurisdiction."* Please can ESMA provide clarity with respect to the choice of jurisdiction, on (i) how this should be addressed in relation to Third Countries and (ii) if the EBA Guidelines should prevail on this point.

(h) suggests that the data location should be a country. We believe that this should be amended to allow country or region, which would be in line with paragraph 43g, as well as EBA Guidelines, and would be better where the security of the data could be compromised by disclosing too much information, such as a specific geographical location. Furthermore, the requirement to document the location of the data processing goes beyond the corresponding requirement in EBA Guidelines paragraph 54(h), so we request alignment with the EBA language.

(l) the requirement to document the location of the data processing goes beyond the corresponding requirement in EBA Guidelines paragraph 54(h), so we request alignment with the EBA language.

We note that ESMA has not stipulated the register requirements for non-critical/important cloud outsourcing arrangements, whereas the EBA has set detail on this. This may leave room for National Competent Authorities (NCAs) to adopt an approach which deviates from

those set out by the EBA which could result in an inconsistent register regime between non-critical/important cloud outsourcing under the approach of the EBA and ESMA for those dual regulated firms.
<ESMA_QUESTION_COGL_2>

Q3 : Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

<ESMA_QUESTION_COGL_3>
AFME would like to raise the following:

Paragraph 33 appears to go further than the EBA Guidelines, which as we have outlined above will be problematic for firms who are subject to both. If it is to be retained, we note that some of the items called out, such as interoperability and data portability, may well be particularly challenging, or in some cases not possible.

Furthermore, we suggest that firms should be able to make their assessment based upon what they can reasonably be expected to know. For example, in assessing item vii on possible concentration risks, firms are not likely to have visibility of sectoral concentration risks.

If concentration risk is to be assessed within the sector, we believe that this should be done directly by authorities. For risks of this nature, authorities (e.g. supervisory bodies) are well positioned to have oversight at an industry level, as compared to FIs individually. Financial institutions should be able to leverage the certainty provided by this oversight of critical CSPs by authorities, which at the same time would make more efficient the due diligence process for these providers, rather than requiring each individual financial institution to perform their own assessments. We believe, however, that any such assessment should not restrict the choice of outsourcing arrangements or providers available to firms. The focus should be on reducing the risks arising from concentration rather than reducing concentration itself which we believe would be difficult and require undesirable sacrifices to security, efficiency and innovation.

In terms of an assessment of possible concentration within the firm caused by multiple cloud outsourcing arrangements with the same CSP, we would emphasise that firms should be able to undertake this as an internal assessment, based on risk appetite, and not be mandated to assess this on stipulated metrics that are set in regulatory guidance. Any such metrics would struggle to account for the range of business models and outsourcing arrangements across the industry.

We welcome that the Guidelines recognize in paragraph 35 the possibility for financial institutions to use certifications based on international standards and external or internal audit reports which will also facilitate the due diligence process of CSPs. Furthermore, there needs to be some flexibility to adapt implementation after the contract stage, since a firm's plans and understanding can change once it has more experience of working within CSPs systems and processes.

In relation to paragraph 36 on reassessment, we note that the risk to a firm posed by an outsourcing arrangement is more likely to change rather than the criticality of the function being outsourced. Similarly, an organisational change at a CSP, or material sub-outsourced services provider, may also not be significant, as it would not change the materiality of the outsourced service. We also note that the assessment is required to take into account a material change in relation to the nature, scale or complexity of the risks inherent to the cloud outsourcing arrangement. While we recognise this requirement, we wish to clarify that the scaling up of use should not be considered synonymous with the scaling up of risk to the firm. Taking the example of load balancing, use of the outsourced service could scale rapidly

to meet demand, but this would already be accounted for in contractual arrangements, due diligence and risk assessment and therefore may not warrant a reassessment of materiality or criticality.

<ESMA_QUESTION_COGL_3>

Q4 : Do you agree with the proposed contractual requirements? Please explain.

<ESMA_QUESTION_COGL_4>
AFME would like to raise the following:

In relation to the items to be included in the written agreement under paragraph 41, we request that these are aligned with the requirements in the EBA Guidelines (paragraph 75) as well as with other requirements such as the EBA Guidelines on ICT and security risk management[4]. Divergence between the ESMA and EBA requirements increases the implementation complexity for firms.

For example, we note that under 41k, specific mention of provisions regarding management of incidents by the CSP, and the obligation for the CSP to report incidents, should be aligned with the EBA Guidelines on ICT which set that contracts and service level agreements should include operational and security incident handling procedures including escalation and reporting (paragraph 8.b). It is also unclear how detailed those expectations are, and whether compliance with external standards such as the Cloud Security Alliance Cloud Control Matrix[5] or ISO security standards[6], would be sufficient.

Similarly, under 41(c), *"the governing law of the agreement and, if any, the choice of jurisdiction"*, we request the same clarity as for 29(g) above - on (i) how this should be addressed in relation to Third Countries and (ii) whether the EBA Guidelines should prevail on this point.

<ESMA_QUESTION_COGL_4>

Q5 : Do you agree with the suggested approach regarding information security? Please explain.

<ESMA_QUESTION_COGL_5>
AFME would like to raise the following, noting that ESMA has diverged from the EBA Guidelines in a number of places which, as outlined above, it likely to be problematic for firms subject to both:

In paragraph 43c, we suggest that it may be appropriate in some cases for encryption keys to be stored using CSP key management capabilities. For example, some firms may determine that using the storage services of a CSP may presents less risk in comparison to internal key management capabilities. In addition, in some cases keys might be stored by the CSP until the provider develops a technical solution. The example provided in 43c. should therefore be removed.

Overall, we recommend that the guidelines on information security are fully aligned with the November 2019 EBA Guidelines on ICT and security risk management[7], where appropriate. This will reduce the regulatory fragmentation, and compliance burden, for firms which will be subject to both. For example, consistency in matters related to encryption and key management.

[4] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[5] https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix
[6] E.g. ISO 27001, 27002 and 27018, as existing industry standards and certifications for supervisory requests.
[7] https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management

We also support ESMA's lack of prescription in relation to the use of encryption keys, noting that firms should have the ability to consider their own appropriate use of encryption tools and key management solutions and to choose the best solution for the security and integrity of their data.

Finally, we note that the guidelines for information security as listed are only a subset of requirements that firms may consider when assessing cloud outsourcing or monitoring existing compliance on an ongoing basis. Equally, the pace of change in technology and security may increase or decrease the importance of some of these areas over time. We therefore request that the Guidelines should not unintentionally lead to specific preferred solutions in the industry or prevent firms from certain cloud outsourcing arrangements due to their specificity as drafted.

<ESMA_QUESTION_COGL_5>

Q6 : Do you agree with the suggested approach regarding exit strategies? Please explain.

<ESMA_QUESTION_COGL_6>
AFME would like to raise the following noting that ESMA has diverged from the EBA Guidelines in a number of places which, as outlined above, it likely to be problematic for firms subject to both:

While exit strategies are critical, we are concerned that that the exit strategy guidance as currently drafted is overly prescriptive and does not allow firms to distinguish between CSP arrangements. For example, firms' exit strategies should be tailored to the specific outsourcing arrangement e.g. a large vs small CSP, an intragroup vs external CSP. As noted in the current IOSCO outsourcing consultation, the risks associated with outsourcing tasks to an affiliated service provider may be different from those encountered in outsourcing to an unaffiliated external service provider. A regulated entity may have the ability to control or influence the actions of the affiliated service provider, and the regulated entity may be more familiar with the affiliated service provider's business attributes. These factors might reduce certain risks involved in outsourcing compared to outsourcing to an unaffiliated service provider.[8] We also note that any requirement to ensure transition plans to an alternative provider would, in the case of an outsourcing to an affiliated provider, leave firms with little option but to rely on external third-party providers. We do not believe this is in line with the policy objectives of ESMA.

We further note that some CSPs (e.g. smaller national or regional specific providers) may pose a far lower volume or business continuity risk, which should not require testing of the exit strategy. Therefore, there should be flexibility for firms to determine the extent to which testing, and what type, is appropriate for each arrangement.

Finally, where multiple services are outsourced to the same CSP, the exit or contingency plan may be most appropriate at an overall group level, rather than having individual plans for each specific service or for each specific legal entity within the group. In fact, plans developed on a legal-entity basis may reduce the effectiveness of resilience planning by the group.

<ESMA_QUESTION_COGL_6>

Q7 : Do you agree with the suggested approach regarding access and audit rights? Please explain.

<ESMA_QUESTION_COGL_7>

[8] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf at page 12

AFME would like to raise the following:

While AFME broadly agrees with the approach, we would appreciate authorities' support in increasing the use of certifications and external and internal audit reports made available by the CSP, and pooled audits. The performance of CSP audits can be particularly costly and resource intensive.

In addition, as mentioned in Q3, in case of CSPs that become critical for the financial sector, we believe that authorities (e.g. supervisory bodies) would be better positioned to audit CSPs at an industry level, as compared to FIs individually. This would help to make the process more efficient rather than requiring each individual financial institution to perform their own assessments, reports, and controls. We would welcome ESMA's engagement with the industry on this topic, particularly given ESMA's convening power. At the moment, however, our understanding is that it would be down to individual firms to determine what type of pooled audit or third-party certification would be sufficient.

We note that the access and audit rights set out in Guideline Six are not described as "full" and "unrestricted", as set out in paragraph 87 of the EBA Guidelines.
Similarly, we note that paragraph 53 of the ESMA Guidelines does not include the following statement in bold that is mentioned by the EBA:

> "Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities should provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation **or would lead to a situation where the audit would no longer be effective**."[9]

We would suggest that this sentence is replicated by ESMA in its final guidelines.
<ESMA_QUESTION_COGL_7>

Q8 : Do you agree with the suggested approach regarding sub-outsourcing? Please explain.

<ESMA_QUESTION_COGL_8>
AFME would like to raise the following:

Confirmation of what constitutes a 'material change' (paragraphs 55d-f) that warrants CSPs to advise firms of would be useful, as well as how far down a sub-outsourcing chain a firm is expected to analyse.

Furthermore, we would appreciate ESMA's views on what would be considered a sufficient notification period (i.e. to notify a CSP of the request to conduct a risk assessment) and duration allowed for a firm to carry out a risk assessment.

We also wish to highlight the complexity of the right to object to an intended sub-outsourcing where this may indirectly impact many firms. Whilst the right to object may benefit a firm in meeting their regulatory and compliance obligations, one firms objection to a CSP sub-outsourcing may also impact on other firms who do not share the same objection, or prefer that the sub-outsourcing change is permitted. We request ESMA to consider how this obligation may manifest within the industry to ensure sufficient transparency and a level-playing field for firms use of cloud outsourcing.

<ESMA_QUESTION_COGL_8>

[9] Paragraph 95 of the EBA Guidelines

Q9 : Do you agree with the suggested notification requirements to competent authorities? Please explain.

<ESMA_QUESTION_COGL_9>
AFME would like to raise the following:

It is common practice for multiple services to be outsourced to a single CSP (for example when using Infrastructure as a Service). We request clarification that, in such situations, it is not required to notify the competent authority when an additional services are onboarded to the same CSP, i.e. that the notification should be an overall relationship level, rather than at the individual service and/or application level.

Firms continue to struggle with pre-approval requirements in some jurisdictions. While recognising the necessity of providing adequate notification to authorities, we believe that explicit pre-approval requirements are a barrier to financial institutions in attempting to keep up with innovation and competition from other sectors. The treatment of the notification process as a form of pre-approval request means that firms must wait to implement their proposed outsourcing, often without a clear sense of even how long the response time from the Competent Authority might be (of whether it might instead be considered, after a period, a case non-objection).

We therefore encourage ESMA to clarify that the notification process is not meant to represent a pre-approval or prior-authorisation regime. We believe that this needs to be stated clearly in these guidelines to avoid different interpretations that competent authorities might make and to ensure harmonisation across the EU.

In relation to notification timelines, we request clarity from ESMA as to whether this may be in line with the firm's outsourcing lifecycle framework, mutually agreed with the local Competent Authority.

<ESMA_QUESTION_COGL_9>

Q10 : Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

<ESMA_QUESTION_COGL_10>
Yes, noting our comments above on authorities supporting the industry in the use of certifications and audit reports, and pooled audits, as well as on a potential oversight framework for critical CSPs. We also encourage competent authorities to discuss their findings on concentration risk with firms and not to put in place any measures that restrict firms in their choice of CSP or outsourcing arrangement.

<ESMA_QUESTION_COGL_10>

Q11 : Do you have any further comment or suggestion on the draft guidelines? Please explain.

<ESMA_QUESTION_COGL_11>
Yes, we wish to raise the following:

We request that ESMA aligns its definitions with those in the EBA Guidelines (and more generally aligns requirements at a global level where possible) to avoid unnecessary complexity for firms that are subject to both set of Guidelines and would be unable to comply with both if they are different.

If full alignment between the EBA and ESMA cannot be achieved, then we request confirmation that (for entities in scope of both EBA and ESMA requirements) compliance with the EBA Guidelines would be seen as substituted compliance. However, we note that this approach is not ideal as it leaves open the possibility than individual national competent authorities might create their own requirements based on elements of each set of Guidelines, which would further increase implementation complexity for firms.

In relation to areas where alignment of definitions would be needed:

Cloud outsourcing arrangement: Section 3.2 Definitions in the CP proposes that "cloud outsourcing arrangement means an arrangement of any form, including delegation arrangements, between: (i) a firm and a CSP by which that CSP performs a function that would otherwise be undertaken by the firm itself; or (ii) a firm and a third party which is not a CSP, but which relies on a CSP (for example through a sub-outsourcing chain) to perform a function that would otherwise be undertaken by the firm itself. In this case, a reference to a 'CSP' in these guidelines should be read as referring to such third party."
While this proposed definition of outsourcing arrangement largely mirrors the approach of the EBA, we note that the EBA's GLs provide further clarification that a service should be provided on a 'recurring or ongoing' basis. Specifically, the EBA GLs note in paragraph 26 that:

> *"Within this assessment [of whether the arrangement is considered outsourcing], consideration should be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by institutions or payment institutions, even if the institution or payment institution has not performed this function in the past itself*."

A similar clarification is not provided by ESMA. Therefore, under the current ESMA draft CP, a one-off or single service could be subject to the strict requirements on cloud outsourcing. However, such non-ongoing services can have a significantly reduced risk profile and do not require ongoing management as does a recurring arrangement. Therefore, we request the addition of the text set out above, as the current drafting of the supervisory statement appears overly broad.

Furthermore, it may be helpful for ESMA to consider including a catalogue of examples of cloud arrangements which should, or should not, be considered as outsourcing. This is the approach taken by, for example, the Monetary Authority of Singapore[10] or the Australian Stock Exchange[11], and we feel that it provides helpful clarity for firms.

Private cloud: ESMA has defined private cloud with reference to a model where "cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer". This contrasts with the EBA definition (paragraph 12) which notes that private cloud is "cloud infrastructure available for the exclusive use by a single institution or payment institution". The EBA definition is preferable because it leaves open the possibility that the cloud infrastructure can be owned and operated entirely by the consuming firm whereas the term customer implies a third-party relationship.

The use of 'customer' also creates confusion because it does not acknowledge the range of possibilities within the private cloud deployment model. The inclusion of customer also leaves it open for NCAs implement their own interpretation of the term and could lead to the

[10] https://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

[11] https://www.asx.com.au/documents/rules/asx_clear_guidance_note_09.pdf

need for firms to document more granular detail on their private cloud arrangements. In addition, 'control' is also an ambiguous term in this context because, as with 'consumer', it covers a range of possible practices depending on the nature of a firm's private cloud deployment.

For example, customer could be interpreted to be at the line of business level (or the application level) within each legal entity which would become burdensome for firms to adhere. Equally, control could be taken to imply a firm needed to maintain on-premise control of the private cloud infrastructure rather than logical separation from other users of the third-party provider's service.

Cloud and Cloud Service: As above, we recommend that ESMA adopts the same definition as EBA, emphasising the points made above in relation to firms that are both EBA and ESMA regulated.

Intragroup arrangements: The EBA Guidelines in paragraph 43c also allow firms to differentiate intragroup and external outsourcing arrangements. While each arrangement should be assessed on its specific risk profile, we do not believe that it is ESMA's intention to capture, for example, the head office of a group as a third-party service provider. Similarly, we suggest that specific reference should be made to the exclusion of internal virtualisation or private cloud solutions.

Finally, the definition of 'cloud outsourcing arrangement' states in part ii that 'CSP' should be understood also to cover third parties which rely on CSPs, for example as part of a sub-outsourcing chain. We are concerned by this expansion of the term. Third parties may use cloud for a variety of purposes, often in way which is unconnected to the outsourcing service. The definition also has the potential to capture intra-group arrangements. We therefore suggest that this definition is refined to remove this clause, or that further examples are given as to the types of arrangement which are not intended to be caught by this definition.

<ESMA_QUESTION_COGL_11>

Q12 : What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organization, where relevant.

<ESMA_QUESTION_COGL_12>
As highlighted in our responses to the other questions in this consultation, we would support close alignment between these guidelines and the EBA Guidelines, towards compliance with which the industry is already working. This would significantly reduce the level of resource required for implementation and compliance with these guidelines as a standalone item.

<ESMA_QUESTION_COGL_12>