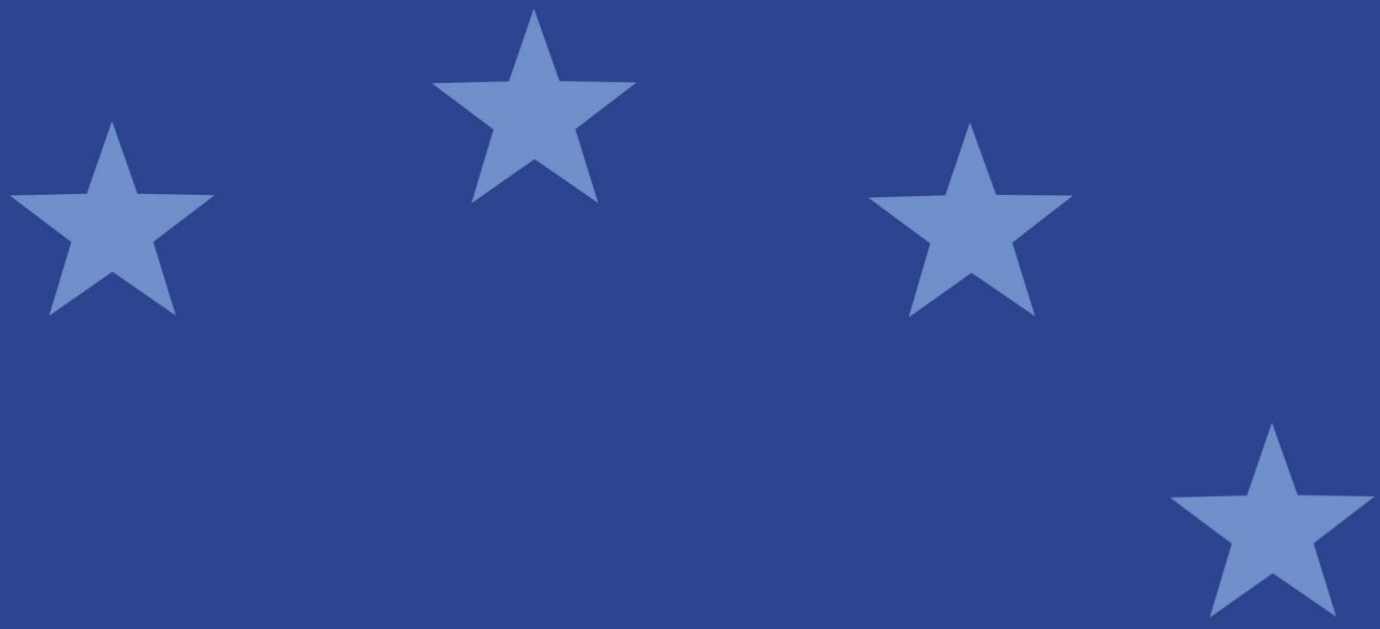
esma European Securities and Markets Authority

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. 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	European Banking Federation
Activity	Banking sector
Are you representing an association?	☒
Country/Region	Belgium

Introduction

Please make your introductory comments below, if any

<ESMA_COMMENT_COGL_1>

The European Banking Federation (EBF) welcomes the chance to comment on the ESMA Guidelines on Outsourcing to Cloud Service Providers (herafter ESMA GL).

Looking at the already published EBA Guidelines on outsourcing arrangements (hereafter EBA GL) from 25 February 2019, European banks already face a dedicated set of requirements for outsourcing, including cloud computing services. Implementation of the GL by the national competent authorities in European member states provides the framework for banks' cloud adoption. In turn, we consider it of **outmost importance to provide banks with a consistent supervisory framework**, avoiding diverging requirements across the EBA and ESMA GL. There should be one single set of rules (ESMA and EBA). To avoid administrative burden and disproportionate effects on dual regulated firms under both sets of GL, European banks encourage an explicit reference in the ESMA GL that banks which are compliant with the EBA GL requirements should also be considered compliant by the national competent authority in regard to the ESMA GL. We invite ESMA to consider the respective example of a reference in EIOPA Guidelines on outsourcing to cloud service provides (February 2020), Introduction para. 4.

We welcome ESMA's understanding that the main risks associated with cloud outsourcing are similar across sectors. ESMA has considered the recent guidelines published by EBA and EIOPA. However, we have identified a number of details within the ESMA GL where presentation and/or details of the requirements in question deviate from the established EBA GL. In the following comments, we invite ESMA to reconsider the identified deviations and to stronger align with existing EBA requirements. Where considered helpful, further examplaratory guidance – in turn required to be aligned with EBA GL – is suggested. Such alignment will prevent detrimental burdens for banks (e.g. in terms of time and work effort,

respective costs) by allowing a streamlined compliance with both EBA and ESMA supervisory framework. A fragmented approach will otherwise be difficult for firms who are regulated by both the EBA and ESMA, ultimately imparing on the ability to adopt cloud seamingless at scale.

Where such alignment would not be completely achieved, we request confirmation by ESMA that (for entities in scope of both EBA and ESMA requirements) compliance with the EBA Guidelines would be seen as substituted compliance.

We encourage ESMA to consider the points made in the following answers as a positive contribution in the spirit of ESMA Regulation 1094/2010, e.g. Art 2(3), stating that "The Authority shall cooperate regularly and closely with the ESRB, as well as with the European Supervisory Authority (European Banking Authority) and the European Supervisory Authority (European Securities and Markets Authority) within the Joint Committee and shall ensure cross-sectoral consistency of work and the establishment of common positions in the area of supervision of financial conglomerates and on other cross-sectoral issues."

A maximum alignment of ESMA GL to the pre-existing EBA GL will help to support financial institutions covered by both regimes in the complex process of cloud adoption under the strict financial regulatory framework. Serving the consumer demands in times of digital transformation, safety and regulatory compliance are of key importance to European banks. In turn, we appreciate legal certainty and avoidance of disproportionate burden by means of GL alignment on cloud outsourcing.
<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>

We encourage a stronger alignment with the EBA GL on the following points.

Structure and focus of the ESMA GL' segments could leverage stronger the EBA GL, allowing banks to operate within an established set of GL sections. Such simple assistance for navigation and orientation would help to limit the workload by the necessary implementation of the requirements into banks' compliance processes. In respect of ESMA's dedication to consider the EBA GL to address "similar main risks across sectors", we perceive such editorial alignment to be beneficial and without any impairment on ESMA's approach.

We recommend an alignment of ESMA's proposed definition with EBA GL para. 26 to 31. It is crucial to provide the sectors with an equally clear understanding of the applicable definition of cloud as part of outsourcing. We suggest to follow EBA's approach of

including list of examples as part of the guidance. Concretly, we recommend to include a list of exceptions of services not being considered cloud outsourcing, as laid out by EBA GL para. 28.

We suggest to clarify within the given ESMA definition of 'cloud outsourcing arrangement" that rules apply to cloud services in the range of investment services only. It would be helpful if the definition could further clarify that not all Cloud Service Providers (CSPs) activities are automatically outsourcing, considering the diverse and continuously developing field of activities of BigTech/CSPs. For more suggestions regarding definitions please consider the answer to Q.11 below.

ESMA GL 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. EBA GL 54 states that an explanation is required only for why an outsourced function is considered critical or important. Considering the number of foreseen non-critical functions, expected to develop further over time in line with technological innovation, the negative explanation why something is non-critical – rather than critical – appears disproportionally burdensome for financial institutions. In line with the established risk-based approach by both EBA and ESMA, the requested explanation should only focus on why an outsourced function is considered critical or important. Again applying the principle of proportionality, firms should clarify their respective criteria only once to the regulator, afterwards standing ready to fullfill later information requests on specific functions on demand.

We encourage ESMA to include examples under Guideline 1.27, reflecting the monitoring of CSPs by firms via a risk-based approach. Such examples should pick up on security measures and adherences to agreed service levels for outsourcing of critical or important functions. Firms' organization of monitoring can directly benefit from such additional ESMA guidance by examples (enhanced clarity).

In order to secure a strong alignment of ESMA with the EBA GL, we invite ESMA to consider including a reference to actions in case of material changes/severe events regarding outsourcing arrangements, as lied out by EBA GL para. 59.

<ESMA_QUESTION_COGL_1>

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

<ESMA_QUESTION_COGL_2>

1.Register

We welcome the acknowledgment of EBA GL para. 53 to 56 regarding an outsourcing register. The importance of such register is reflected by proactive and cross-industry work of the EBF Cloud Banking Forum, based on the EBA GL. It offers technical guidance to national supervisors, CSPs and banks by means of a register template (download here). However, ESMA now also aims for a record of terminated cloud outsourcing arrangements for an appropriate period of time in accordance with local law (Guideline 1.28). We encourage ESMA to elaborate on the reason for such additional requirement, considered that terminated arrangements do not play into the actual existing risk under the risk-based approach to cloud adoption and supervision.

As reflected by the EBF's dedication to a harmonized application of the register guidance fields (see above mentioned template), it is important for financial institutions to face a consistent set of register requirements, allowing to provide the necessary information under a risk-based approach. However, ESMA Guideline 1.29 introduces additional fields compared to the EBA GL. Forcing banks to create and maintain different register sets for cloud outsourcing (and outsouring under EBA GL beyond cloud) creates disproportionate burden for the firms. We call upon ESMA to align the register fields with the EBA register. The latter sufficiently reflects the risk-based approach, offering necessary information on cloud outsourcing. A single set of requirements, as established by EBA, serves sufficiently well. Hence, we encourage a close alignment.

Should ESMA nevertheless feel a need for the register deviations, we invite it to provide more clarity – e.g. examples on the points indicated below – on why and how these register fields should be provided additionally to/different from today's EBA register:

a. **Guideline 1. 28:** Brief summary of rationale for critical classification to be included
b. **Guideline 1.29 (e):** *'whether the outsourced critical or important function supports business operations that are time-critical'*.
   We welcome ESMAs view as to whether a recovery time threshold, criticality rating and or RRP rating would suffice.
c. **Guideline 1.29 (f)** "*name and brand name*" of provider
d. **Guideline 1.29 (g):** *"the governing law of the cloud outsourcing arrangement and, if any, the choice of jurisdiction."*
   We encourage 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 GL are intended to prevail on this point.
e. **Guideline 1.29 (h):** Confirm data processing location (in addition to data transfer/storage)
f. **Guideline 1.29 (i):** "…names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the countries where the sub-outsourcers are registered, where the sub-outsourced service will be performed, where the data will be stored and where the data may be processed;"
   We invite ESMA to provide examples.
g. **Guideline 1.29 (m)** *"the estimated annual budget cost, excluding VAT, of the cloud outsourcing arrangement"*.
   EBA GL para. 54, 55 does not explicitly exclude VAT. A diviation between the different GL creates detrimental burden for firms' reporting procedure, introducing an unnecessary chance for confusion. At the same time, it introduces complications in the reporting due to changing VAT rates. The current Covid-19 crisis has shown that Member States can use VAT rates to address challenges to the economic situation. The ESMA requirement incorporates these fluctuations and corresponding complications then in the reporting process without laying out the intended benefit. We invite ESMA to align with EBA, not raising VAT exclusion. At a minimum, we kindly request

ESMA to please share if it has any objections to receiving data which includes VAT, as long as this fact is indicated clearly and demonstrates the calculation.

Additionally,we invite ESMA to ensure alignment with EBA register requirements in para. 53 and 54 regarding non-critical functions. ESMA Guideline 1.29 does only focus on critical or important functions. The resulting lack of guidance for national competent authorities on non-critical functions – different from the EBA approach – creates the danger of diverging interpretation and resulting supverisory fragmentation. We recommend a consistent register regime between non-critical/important functions and critical/important ones, avoiding legal uncertainty and disproportionate burden for double regulated firms under both EBA and ESMA GL regime.

2.Notification

We encourage ESMA to align the outsourcing notification to the EBA GL' approach. A notification requirement to the competnent authority "in case of planned outsourcing of critical or important functions" in a timely manner appears disproportionaly burdensome, considering the number of cloud arrangements and the existing outsourcing register. We consider the notification of competent authorities sufficiently covered under the EBA GL, without a need to introduce additional requirements regarding the timeframe. Rather than providing helpful guidance, this deviation from the EBA GL carries the danger of supervisory fragmentation across Europe on the matter.

We encourage ESMA to amend its written notification requirements under Guideline 8.58 (content to be reported) to reflect only the information maintained within the obligatory register (Guideline 1.29). Taking into account the risk-based approach, it appears disproportionate to request firms to include two separate lists of information requirements, both to be included – and continuously maintained – within their compliance and reporting processes.

<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>

If concentration risk is to be assessed within the sector, we believe that this should be done directly by competent authorities. For risks of this nature, these authorities (supervisory bodies) are well positioned to have oversight at an industry level, as compared to firms individually. 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, firms should be able to undertake this as an internal assessment, based on risk appetite. Firms should not be mandated to assess it 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.

In addition, we welcome that ESMA recognized in Guideline 2.35 the possibility for financial institutions to use certifications based on international standards and external or internal audit reports. We believe that being able to use these tools will contribute to making the CSP due diligence process more efficient.

Looking at the EBA GL, ESMA Guideline 2.33 appears to emphasize ICT and information security risks, and oversight limitations for the firm arising from:

a. Selected cloud service and proposed deployment models
b. Migration and/or implementation processes
c. Sensitivity of function and related data and security measures
d. Interoperability of systems and applications of the firm and the CSP
e. Data portability between firm and CSP

We welcome ESMA to provide scenarios/examples on how compliance can be reached in relation to the above. Such additional guidance would help to avoid diverging interpretation in Member States throughout the implementation process of the GL.

We encourage ESMA to align Guideline 2.36 ("*A firm should reassess the criticality or importance of a function previously outsourced to a CSP periodically* [.]") to the EBA GL Title 2 Section 4. Its para. 31 e) targets the aggregated exposure and potential cumulative impact. The introduction of a peridodical review process, indepent from the service in questions and without room for the firms to adjust the interval to the risk-profile of the function, can be a disproportionate burden.
<ESMA_QUESTION_COGL_3>

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

<ESMA_QUESTION_COGL_4>
In order to facilitate needed harmonization of requirements for double regulated firms, we invite ESMA to align Guideline 3.41 with the requirements in the EBA GL para. 75. Even slight diviations in the wording trigger complex reassessments within dual regulated firms (due diligence and compliance processes) and hence create disproportionate burden. Where ESMA Guideline 3.31 (c) is calling for inclusion of "the governing law of the agreement and, if any, the choice of jurisdisdition", we invite ESMA to elaborate on this choice, providing guidance on how financial institutions are expected to include this information in the contract for CSPs' – potentially partial – service provision in third countries.

European banks appreciate the explicit clarification under ESMA GL 3.41 f) regarding data storage and processing (targeting the location of data centres).
<ESMA_QUESTION_COGL_4>

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

<ESMA_QUESTION_COGL_5>
We encourage ESMA to align Guideline 4.43 with requirements under EBG GL section 13.2. There is no need for additional codification of minimum requirements beyond the EBA GL, since such prescriptive requirements would rather complicate the risk-based approach of institutions to assess the criticality of functions.

Where ESMA provides additional requirements, we encourage a concretization of the guidance by example-scenarios, leaving no room for national fragmentation during the later implementation process. We encourage ESMA to clarify the application of newly introduced and advanced criteria to financial institutions that are already regulated under the EBA GL as well as under the EBA guidelines on ICT and security risk management. A diverging regime on information security would establish a disproportionate burden for firms, requiring workload- and cost-intensive procedures.
Considered additions by ESMA:

a. **Guideline 4.*43* (a):** *Information security organisation* – clear allocation of information security roles and responsibilities between firm and CSP, especially with regard to threat detection, incident management and patch management.
b. **Guideline 4.*43* (b):** *Access management* – strong authentication mechanisms (e.g. two factor) are implemented and access controls prevent unauthorised access to firm's data and back-end cloud resources
c. **Guideline 4.*43* (d):** *Operations and network security* – consider appropriate levels of segregating networks (e.g. tenant isolation in shared cloud environment) and processing environments (e.g. text, UAT, development, production)
d. **Guideline 4.*43* (e):** *APIs* – consider integration (CSP to firm system) mechanisms to ensure security of APIs (e.g. Information security policies and procedures for APIs)

Considered clarifications by ESMA:

a. **Guideline 4.*43* (c):** *Encryption and key management* – consider use of encryption technologies where appropriate for data in transit, memory, at rest and back-ups, in combination with appropriate key management solutions to limit non-authorised access to encryption keys
b. **Guideline 4.*43* (f):** *Business continuity and disaster recovery* – controls should be in place (e.g. setting minimum capacity requirements,

selecting hosting options that are geographically spread, replicating machine images to an independent storage location)

c. **Guideline 4.*43* (g):** *Data location*_ - adopt risk based approach to data storage and processing (namely country and region)
d. **Guideline 4.*43* (h):** *Compliance and monitoring* – ensure CSP complies with internationally recognised information security standards and has implemented appropriate security controls (e.g. requesting CSP to provide evidence that it conducts relevant information security reviews and performing regular assessments and tests of CSP information security)

<ESMA_QUESTION_COGL_5>

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

<ESMA_QUESTION_COGL_6>
We appreciate an alignment of ESMA Guideline 5 with the EBA GL Section 15 on exit strategies. Regarding the testing of exit plans under ESMA GL 5.44 a), we would like to emphasise the necessary risk-based approach. In terms of recommended testing (incl. considerarions of appropriateness) we would like to draw attention to the EBF Cloud Banking Forum's cross-industry technical guidance paper "Cloud exit strategy – testing of exit plans" (download here).
<ESMA_QUESTION_COGL_6>

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

<ESMA_QUESTION_COGL_7>
We encourage ESMA to align Guideline 6 with EBA GL section 13.3 on access, information and audit.
EBA GL para. 87 provides relevant guidance for supervisors to approach the issue of auditing. The EBF welcomes a risk-based approach. We do not see a need for additional requirements under ESMA 6.51 (a) ("*ensures that the scope of the certifications or the audit reports covers the CSP's systems (for example processes, applications, infrastructure, data centres), the key controls identified by the firm and the compliance with the relevant legal requirements*") and 6.53 (for prior notification for on site visits: "*Such notice should include the location, purpose of the visit and the personnel that will participate to the visit.*"). Accordingly, ESMA is invited to align its considerations and add the important descriptions of required access to CSPs as being "full" and "unrestricted", in line with EBA GL para. 87.
ESMA GL 6.53 should be aligned with EBA GL para. 95, replicating the limitation of notifications for on site visits if this "*would lead to a situation where the audit would no longer be effective*".
<ESMA_QUESTION_COGL_7>

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

<ESMA_QUESTION_COGL_8>
Regarding the information fields under the register (Guideline 1.29) and notifications, please see answer to Q2.

We consider it helpful if ESMA could – in alignment with existing EBA GL references – provide firms with further guidance on intra-group outsourcing constellations in case of sub-outsourcing. The EBA GL include simplifications for groups. These refer, for example, to central exit plans, central business continuity plans, central outsourcing management, central outsourcing register or existence of a waiver according to Art 7 CRR. We would appreciate it if the ESMA GL would also take this into account, considering the existing supervisory attention and responsibitlities for intra-group constellations.
<ESMA_QUESTION_COGL_8>

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

<ESMA_QUESTION_COGL_9>
For comments on notification requirements please consult also the answer to Q2.

Additionally, we invite ESMA to clarify in Guideline 9 that the actions and targeted satisfaction of national competent authorities is not an invitation for pre-approval requirements in the individual jurisdiction. A formalized pre-approval process proves to be a barrier to fast adoption of innovative technology. Driven by competition – increasingly cross-sectorial as shown by large online platforms and their respective data and infrastructure advantages – the required speed of innovative tech applications in financial institutions has been increased. European banks remain dedicated to serve both their customers' expectations (of increasingly fast tech solutions) and their responsibilities under the financial regulatory framework. Additional pre-approval processes for cloud outsourcing, making the innovative tech adoption dependent on external workstreams by different public authorities, significantly slow this adoption. Furthermore, different procedural rules of such pre-approval across European jurisdictions would create a significant fragmentation of supervisory requirements and corresponding reaction times. Ultimately, the inherently cross-border cloud potential would be seriously undermined. We believe that the ESMA Guideline 9 provides for the right opportunity to clarify that pre-arrpoval is not expected. Following a risk-based approach under the ESMA GL (same as under the EBA GL), protection of financial stability and accountability remains nevertheless secured in the sectors.
<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>
Acknowledging ESMA Guideline 9 on supverision, we invite ESMA to provide further guidance on Guideline 9.61 a) and b) regarding the details of the processes to be put in place by firms. End-to-end examples could help demonstrating how this should be looked at by NCAs and firms (examples of relevant governance, expected ressources, operational processes)

Guideline 9.62 introduces monitoring in case of identified concentration risk. We invite ESMA to provide further guidance on how comptent authorities should approach firms within this monitoring process and to what extent the authority could share their findings with firms in return. An enhanced information access for firms on the concentration risk assessment by the comptenent authority would provide valuable under the firms' risk-based approach to cloud outsourcing.
<ESMA_QUESTION_COGL_10>

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

<ESMA_QUESTION_COGL_11>
We encourage ESMA to align the proposed definition with definitions included under the EBA GL para. 12.

Specifically, we recommend to include the definition of "Private Cloud" as proposed by EBA. By use of the wording "cloud service customer" (ESMA) instead of "use by single institution" (EBA), the status of a private cloud provider appears to implicate a third-party relationship. Different from public cloud solutions, the private cloud model can be operated by a single firm entirely, excluding third parties. In fact, private cloud deployment models can provide a range of possibilities and should operate under an equally flexible definition. The EBA definition reflects possibilities more easily, avoiding possible confusion in later implementation processes. Additionally, EBA does not include the term "controlled by", which could also trigger misleading – because too narrow – interpretations of privat cloud constellations.
<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>
TYPE YOUR TEXT HERE
<ESMA_QUESTION_COGL_12>