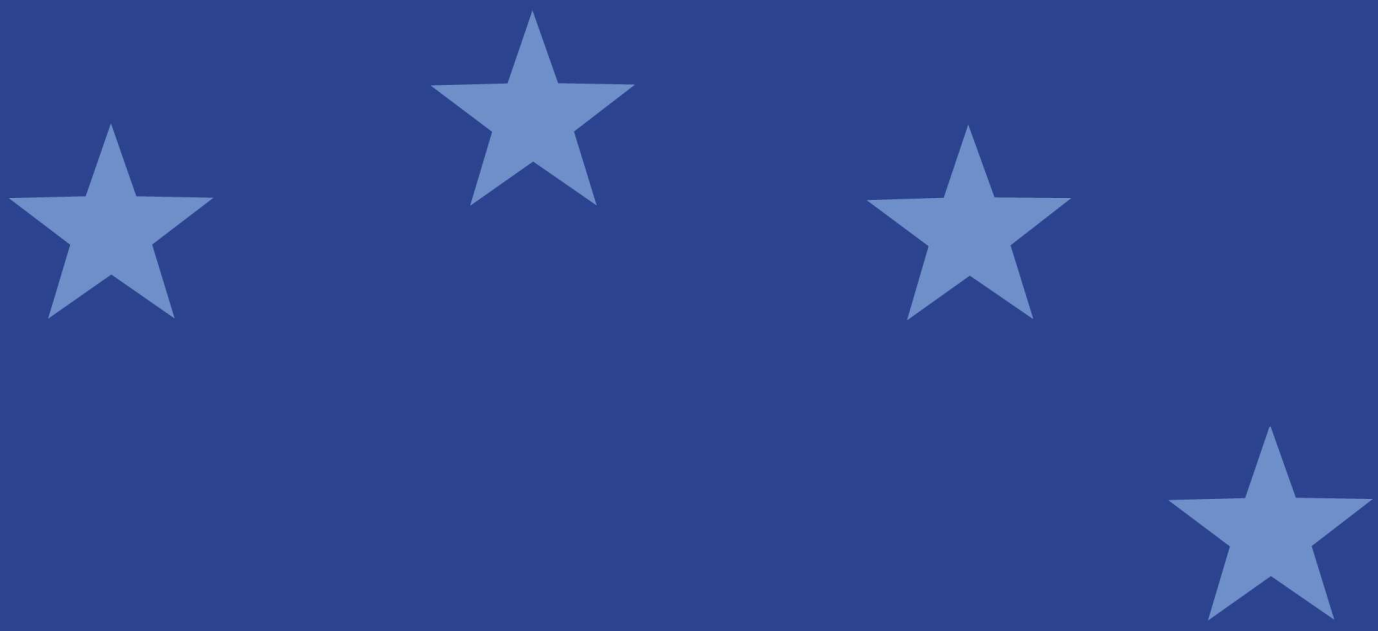
esma European Securities and Markets Authority

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	BlackRock
Activity	Investment Services
Are you representing an association?	☐
Country/Region	Europe

Introduction

Please make your introductory comments below, if any

<ESMA_COMMENT_COGL_1>

1. BlackRock welcomes the Consultation Paper. We restrict our comments (i) to support certain of the core elements of the Consultation Paper and (ii) suggestions for adjustment of certain discrete details.

2. The Consultation Paper's draft guidelines (the "Guidelines") are, in principle, consistent with guidance issued by the EBA and EIOPA. This is positive and provides the industry with certainty.

3. We believe that ESMA should continue to focus its efforts on promoting pragmatic, commercial best practices of (i) diligence, (ii) governance and (iii) corporate systems and controls. **We support a 'principles-based' approach to the risk management of CSPs with risk-based governance and proportionality.** The draft Guidelines, broadly, embody this spirit.

4. BlackRock supports dedicated outsourcing oversight functions as set out in our ViewPoint entitled "The role of third party vendor management" at https://www.blackrock.com/corporate/literature/whitepaper/viewpoint-role-of-third-party-vendors-asset-management-september-2016.pdf. There are numerous vendors providing a wide range of services to asset managers. We support the principle that firms need a vendor management program - and a business continuity management program - that factors in services provided by third parties.

5. Any analysis of CSPs in asset management – by the respective National Competent Authority ("NCA") supervisors – needs to start with an understanding of the different business models of various firms. Each firm has a different

philosophy on which operational functions it wants to control directly versus which functions it wants to outsource. This leads to a very diverse set of operating models across the industry.

6. NCA supervisors should apply the Guidelines based on a detailed understanding of each firm's bespoke operating model, reflecting the precise role that CSPs provide for each respective firm. This means there will be a spectrum – or degrees – of reliance on CSPs be firms dependent on business model. The application of the Guidelines should take account of this spectrum. **Accordingly, we support ESMA's approach to providing the industry with risk-based and proportionate principles when looking to the application of the Guidelines**.

7. While operational functions may be performed by a third party, we support the principle that firms must ensure that CSPs, like the asset manager itself, have sufficient controls to mitigate the risk of operational errors - and to ensure adequate business continuity and disaster recovery plans are in place.

8. We agree with ESMA, in so far as, where a firm has a choice of CSP, conducting due diligence in the selection of CSPs, followed by ongoing monitoring - is key to ensuring that CSPs are adequately managing operational risk and can continue operations, even during times of market stress or business disruptions.

9. BlackRock maintains a selection program with a comprehensive set of guidelines and criteria to ensure that critical providers meet certain requirements without limitations, such as business concentration, financial stability, proper legal documentation, operational efficiencies, and adequate risk mitigation and controls including business continuity plans ("BCP").

10. It is important to recognize that while firms can perform rigorous due diligence on CSPs and engage in a high level of ongoing communication and oversight, firms cannot - and do not - control every aspect of a CSP's functioning. Nor do firms have the ability to guarantee that a CSP will never make a mistake or face an operational or business continuity challenge of its own.

11. Accordingly, we support ESMA's principle that firms should take all reasonable measures – proportionate to the firm's complexity, size and cloud use case – to risk manage firms' relationships with CSPs.

<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>
12. **Guideline 1** states that firms should:

"establish an outsourcing oversight function or designate a senior staff member who is directly accountable to the management body and responsible for managing and overseeing the risks of cloud outsourcing arrangements."

a. The final version of the Guidelines should permit the use of firms' existing governance bodies to satisfy this requirement. Cloud provision is one type of outsourcing arrangement. Its risk management can be administered via firms' existing, mature governance and oversight frameworks.

<ESMA_QUESTION_COGL_1>

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

<ESMA_QUESTION_COGL_2>
No additional comment
<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>
13. **Guideline 2** details (and this repeats across other relevant sections of the Guidelines):

"Where appropriate and in order to support the due diligence performed, a firm may also use certifications ***based on international standards and external*** [emphasis added] *or internal audit reports."*

a. We welcome the pragmatic recognition that the industry will continue to leverage auditing standards - administered by external trades bodies and professional bodies (of chartered accountants, lawyers etc). For example see the SOC 1 and 2 reports, Statements on Standards for Attestation Engagements, produced by the American Institute of Certified Public Accountants Auditing Standards Board and similarly ISAE 3402 – developed by the IAASB.

14. We agree with ESMA that asset managers should take a risk-based approach to ensure that CSP oversight and controls are commensurate with the materiality of the risks posed by the specific cloud provider. We support the Guidelines taking a risk-based approach, for example, in relation to information security measures.

<ESMA_QUESTION_COGL_3>

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

<ESMA_QUESTION_COGL_4>
No additional comment
<ESMA_QUESTION_COGL_4>

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

<ESMA_QUESTION_COGL_5>

15. We agree with ESMA that asset managers should take a risk-based approach to ensure that CSP oversight and controls are commensurate with the materiality of the risks posed by the specific cloud provider. We support the Guidelines taking a risk-based approach, for example, in relation to information security measures as set out below.

> **Guideline 4** details information security requirements. We note the similarities between Guideline 4 and equivalent EBA guidance. We suggest that ESMA considers – for the finalized version of Guideline 4 – that items detailed in paragraphs 43(a)-(h) of the Consultation Paper could be better enacted with a principles-based approach. Rather than being overly prescriptive. ESMA could consider the approach of one of the key principles of the GDPR – that data is to be risk managed securely by means of "appropriate technical and organizational measures". For an example of how this is applied in practice see the ICO Guide at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/#:~:text=At%20a%20glance,and%20physical%20and%20technical%20measures. A principles-based approach can be more effective because information security measures may change over time and would be assessed on the specific use of cloud (including with reference to the sensitivity of the data being processed by a CSP).

<ESMA_QUESTION_COGL_5>

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

<ESMA_QUESTION_COGL_6>
No additional comment
<ESMA_QUESTION_COGL_6>

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

<ESMA_QUESTION_COGL_7>
No additional comment
<ESMA_QUESTION_COGL_7>

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

<ESMA_QUESTION_COGL_8>
No additional comment
<ESMA_QUESTION_COGL_8>

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

<ESMA_QUESTION_COGL_9>
No additional comment
<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>
No additional comment
<ESMA_QUESTION_COGL_10>

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

<ESMA_QUESTION_COGL_11>
No additional comment
<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>
No additional comment
<ESMA_QUESTION_COGL_12>