|  |
| --- |
| Response Form to the Consultation Paper |
| Guidelines on Outsourcing to Cloud Service Providers |

**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](http://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](http://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](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/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 | Fitch Ratings |
| Activity | Other Financial service providers |
| Are you representing an association? |  |
| Country/Region | Europe |

**Introduction**

***Please make your introductory comments below, if any***

<ESMA\_COMMENT\_COGL\_1>

Fitch Ratings (“Fitch”) appreciates the opportunity to review and comment on the Consultation on the topic of Outsourcing to Cloud Service Providers. We set forth below our observations and suggestions regarding the proposals; we have only responded with respect to those elements about which we have comments.

Fitch believes that a clear and consistent set of expectations for CRAs relating to Outsourcing to Cloud Service Providers will advance fulfilment of the CRA Regulation’s objectives. Fitch’s comments aim to ensure that the proposed guidelines are implemented by ESMA in a manner which takes into consideration the activities and characteristics of CRAs and is consistent with the general EU principle of proportionality.

As an overarching drafting comment, Fitch notes that the text of the draft guidelines uses the terminology “cloud outsourcing” and “outsourcing” interchangeably. In order to better align the text of the draft guidelines with their scope, Fitch suggests the consistent usage of the term “cloud outsourcing” throughout the document. Specific references to “outsourcing” within the draft guidelines are highlighted in Fitch’s detailed responses provided below. <ESMA\_COMMENT\_COGL\_1>

**Questions**

1. : 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>

In Fitch’s opinion, it may, for some firms, be appropriate to segregate the responsibility for managing the risks of cloud outsourcing arrangements, for example between a Chief Technology Officer and a Chief Information Security Officer. In order to reflect such a segregation of responsibility, Fitch suggests the following amendment to paragraph 26(c): *“or designate ~~a~~ senior staff member(s) who ~~is~~ are directly accountable to the management body and responsible for managing and overseeing the risks of …”.*

Fitch suggests the following clarification to the text of paragraph 29, part c*): “including the data that is transmitted to the cloud services provider ~~outsourced~~ and whether this data includes personal data (for example by providing a yes or no in a separate data field);”*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraphs 26(c), 27, 28, 29(c), 29(e) and 29(i).

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

Fitch considers the use of reference numbers within the cloud outsourcing register is unnecessary given there are a small number of cloud service providers who can be readily identified by name. It is therefore suggested to remove the requirement contained in paragraph 29(a).

<ESMA\_QUESTION\_COGL\_2>

1. : 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>

In recognition of the inherent limitations in identifying *“all relevant risks”* Fitch suggests the following amendment to the text contained in paragraphs 31(c) and 33(a): *“all ~~relevant risks~~ reasonably foreseeable material risks deemed relevant by the firm”.*

In order to align the text with the scope of the draft guidelines, Fitch suggests the following clarification to the text of paragraph 32: *“the function that the firm intends to outsource to a cloud service provider and the risks inherent to this function.”*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing*” in the text of paragraph 34.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Fitch recognises that the draft guidelines on contractual requirements are closely aligned with paragraphs 74 and 75 of the [EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)](https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1) (“EBA Guidelines”). In general, Fitch considers this high degree of alignment to be a positive factor on the basis that several cloud service providers have publically indicated their willingness to facilitate compliance with the EBA Guidelines. This is relevant given that cloud computing agreements entered into by Fitch (and likely also most other firms) utilise the standard agreements of the cloud service providers and, therefore, the firms’ ability to implement the proposed contractual requirements will largely depend on the CSPs’ willingness to include terms reflecting these requirements in their standard agreements.

In relation to paragraph 41(h), Fitch acknowledges that this text is aligned with the EBA Guidelines, however Fitch anticipates that CSPs may not agree to contractual terms which could give a firm an expressed right to monitor CSPs. Therefore, Fitch suggests that the obligation upon firms to obtain contractual rights enabling the monitoring of CSPs be limited to an evaluation of a CSP based on CSP performance, CSP self-assessment (which will cover performance of activities, the security measures and the adherence to agreed service levels) and, where applicable, audit and certification reports. Fitch believes that such contractual rights would be consistent with the obligations of paragraph 27, which require *“On a risk-based approach, a firm should monitor on an ongoing basis the performance of activities, the security measures and the adherence to agreed service levels by its CSPs.”* Therefore, Fitch suggests that paragraph 41(h) be amended as follows: *“the right for the firm to monitor the CSP’s performance on a regular basis (through an evaluation by the firm of a CSP’s performance, a CSP’s self-assessment and, where applicable, a CSP’s audit and certification reports);”*

In relation to paragraph 41(i), Fitch acknowledges that this text is aligned with the EBA Guidelines, however Fitch highlights that it may not be possible to precisely measure certain aspects of CSP performance, and therefore Fitch suggests the following amendment to the text of paragraph 41(i): *“the agreed service levels, which should, to the extent possible, include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;”.*

In relation to paragraph 41(k), Fitch has not identified a corresponding requirement in the EBA Guidelines and is therefore concerned with the ability of firms to obtain agreement from cloud service providers. Fitch is also of the opinion that many potential cloud service provider incidents would be either (i) immaterial, or (ii) relevant only to individual users. Therefore, Fitch suggests the following amendments to the text of paragraph 41(k): *“provisions regarding the management of incidents by the CSP that can reasonably be expected by the CSP to have a material service impact on the firm’s use of the cloud services, including the obligation for the CSP to report such incidents;”*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraph 41.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

The contents of paragraphs 42 and 43, largely contain additional requirements relative to the EBA Guidelines. Fitch does not anticipate specific issues regarding the implementation of the guidelines in paragraphs 42 and 43. However, Fitch notes that the cooperation of CSPs regarding the implementation of paragraphs 42 and 43 is less tested versus the elements of the draft guidelines which are aligned with the EBA Guidelines.

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraph 43.<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

In relation to paragraph 44(a), Fitch understands that exit plans should be implemented only in the event of the termination of a CSP. Therefore, Fitch suggests the following clarification to the text of paragraph 44(a): *“develop ~~and implement~~ exit plans that are comprehensive, documented and sufficiently tested.”*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraph 44.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

In relation to paragraphs 51(d) and 51(e), Fitch suggests that firms should be able to utilise the auditing party’s internal certification relating to its qualifications, compliance with appropriate standards etc. Fitch therefore suggests that paragraphs 51(d) and 51(e) be deleted and replaced with the following: *“has received certification from the certifying or auditing party (i) with regard to its qualifications or expertise, (ii) with regard to the scope of the audit, and (iii) confirming that the audits are performed according to appropriate standards and include a test of the effectiveness of the key controls in place”.*

Fitch is concerned that the text of paragraph 52 may be understood to impose a requirement upon firms to commission audits (or pooled audits) of cloud service providers. Fitch believes that audit rights should be exercised on a risk-based approach and that user-commissioned audits (or pooled audits) should not be mandatory. Therefore, Fitch suggests the following clarifying amendment to the text of paragraph 52: *“In any case, the firm should assess whether the third-party certifications and external or internal audit reports are adequate and sufficient to comply with its regulatory obligations ~~and, should not solely rely on these certification and reports over time~~.”*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraphs 48 and 51 and *“cloud outsourced”* in place of *“outsourced”* in paragraph 51(g).

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

In relation to paragraphs 55(d), 55(e) and 55(f), Fitch acknowledges that this text is aligned with the EBA Guidelines, however Fitch anticipates that it may be impractical to require CSPs to notify, or seek approval from, firms of planned sub-outsourcing or material changes as such arrangements could relate to overall business development and strategies of CSPs. In our view, a key consideration of sub-contracting is (i) whether a firm has the right to exclude certain parts of the outsourced function from potential sub-outsourcing, and (ii) whether a CSP is taking responsibility for the services performed by its sub-contractors - and these are already addressed under paragraphs 55(a), 55(b) and 55(c). Therefore Fitch suggests deleting paragraphs 55(d), 55(e) and 55(f).

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

Fitch requests clarification, in relation to CRAs, that the notification obligations set out in paragraphs 57 and 58 of the draft guidelines will be satisfied by using the existing *“Template 16: IT Notification Cloud Computing”* of the existing [*Guidelines on Periodic information to be submitted to ESMA by Credit Rating Agencies (ESMA 33-9-295)*](https://www.esma.europa.eu/sites/default/files/library/esma_33-9-295_final_report_guidelines_on_the_submission_of_periodic_information_to_esma_by_credit_rating_agencies.pdf). In order to provide such clarification, Fitch suggests the insertion of the following text into the draft guidelines: *“In relation to CRAs, the notification obligations set out in paragraphs 57 and 58 of these guidelines will be fulfilled by providing Template 16 in accordance with the* [*Guidelines on Periodic information to be submitted to ESMA by Credit Rating Agencies (ESMA 33-9-295)*](https://www.esma.europa.eu/sites/default/files/library/esma_33-9-295_final_report_guidelines_on_the_submission_of_periodic_information_to_esma_by_credit_rating_agencies.pdf)*”.*

As per Fitch’s introductory comment, Fitch suggests to use the term *“cloud outsourcing”* in place of *“outsourcing”* in the text of paragraph 57 and *“cloud outsourced”* in place of *“outsourced”* in paragraph 58(a).

<ESMA\_QUESTION\_COGL\_9>

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

<ESMA\_QUESTION\_COGL\_10>

No response

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

Fitch assumes that firms would not be expected to retrospectively undertake the pre-outsourcing analysis and due diligence activities specified in Guideline 2, in relation to existing cloud outsourcing arrangements. Therefore, Fitch suggests the following amendment to the text of paragraph 17: *“Firms should review and amend accordingly existing cloud outsourcing arrangements with a view to ensuring that they take into account these guidelines (excluding the pre-outsourcing analysis and due diligence activities specified under Guideline 2) by 31 December 2022”.*

<ESMA\_QUESTION\_COGL\_11>

1. : 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 response

<ESMA\_QUESTION\_COGL\_12>