|  |
| --- |
| 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 | Moody’s Deutschland GmbH |
| 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>

Please refer to MIS cover letter.

<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>

***Article 26:***

The Draft Guideline requires that firms *“make sure that the management body has the relevant technical skills.”* This is in the context of a senior staff member having to report directly to the management body on outsourcing to cloud service providers (CSPs) or the firm having to create an outsourcing oversight function. MIS accepts that a regulated entity should have the necessary expertise and resources to adequately implement and review outsourcing arrangements. Many regulated entities require the specific business unit responsible for the outsourcing of a critical or important function to report to the management body at specific intervals, to identify specific risks related to the outsourcing and how these are being mitigated, as well as give an update on the performance of the vendor. This provides an opportunity for the management body to understand how the business is addressing the risk of a particular critical and important outsourcing and to bring this information into its general oversight function. However, this should not be a specific requirement for the management body, nor should outsourcing to the cloud be a specific function that an individual should report on directly to the management body where it is not a critical or important function.

The EBA recognises the principle of general oversight in paragraph 37 of the EBA Guidelines on Outsourcing Arrangements (“EBA Guidelines”)[[1]](#footnote-2) which state: “Institutions and payment institutions should have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and oversight of outsourcing arrangements”. This wording is more proportionate to that proposed in Article 26 and applies the responsibility across the firm and not only to the management body which, in any event, should only be responsible for oversight of a firm’s outsourcing strategy generally.

26. A firm should:

a) …

b) …

c) have sufficient and appropriately skilled resources to ensure appropriate management and oversight of outsourcing arrangements, ~~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. When complying with this guideline, firms should~~ taking into account the nature, scale and complexity of their business and the risks inherent to the outsourced functions ~~and make sure that their management body has the relevant technical skills. Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and control of cloud outsourcing arrangements.~~

***Article 27:***

This Article refers to monitoring the activities of a CSP “*on an ongoing basis*”. This could imply an expectation of real-time monitoring, which would not be in line with the risk-based approach referenced in the Article and throughout the Draft Guidelines. We suggest deleting “on an ongoing basis”.

27. 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. The primary focus should be on the outsourcing of critical or important functions.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

***Article 28:***

Where firms already treat selected outsourcing to CSPs as critical and important, it should not be necessary to duplicate the need for details on determining what is critical or important in a general register on outsourcing to the extent these are maintained by firms in a specific register of critical or important outsourcing. The Draft Guidelines should allow for a materiality threshold as to whether all of the documentation requirements apply. We propose …

28. A firm should maintain an updated register of information on all its critical and important cloudoutsourcing arrangements~~, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. When distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements, it~~ and should provide a brief summary of the reasons why the outsourced function is ~~or is not~~ considered critical or important. ~~Taking into account national law, a firm should also maintain a record of terminated cloud outsourcing arrangements for an appropriate time period.~~

<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>

***Article 32:***

The approach to pre-outsourcing analysis does not sufficiently distinguish between outsourcing of critical and important functions and general outsourcing. The equivalent provision on general outsourcing in the EBA Guidelines[[2]](#footnote-3) requires consideration of only operational risk, whereas the Draft Guidelines additionally require the assessment of legal, compliance and reputational risk. These additional requirements replicate to a large extent the requirements applied to critical and important outsourcing with only limited differentiation to general outsourcing. This would appear to be a disproportionate outcome and risks diluting and confusing the application of a distinct framework for critical and important outsourcing. We propose an amendment to address this ….

32. In general, the pre-outsourcing analysis and due diligence should be proportionate to the nature, scale and complexity of the function that the firm intends to outsource and the risks inherent to this function. It should include at least an assessment of the potential impact of the cloud outsourcing arrangement on the firm’s operational~~, legal, compliance, and reputational~~ risks.

***Article 33:***

While this Article is in reference to critical and important outsourcing, it may not always be necessary or appropriate to undertake all the proposed activity required in the Article. For example, it may not always be necessary to perform a review of the legal system or political stability of another EU member State where pan-EU frameworks are applicable. Including a “where appropriate” into the requirement would provide a firm the necessary flexibility in this regard.

33. In case the cloud outsourcing arrangement concerns critical or important functions, a firm should also, where appropriate:

a) …

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

No comment

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

***Article 43:***

Where possible, the monitoring and compliance function as laid out in this Article should be able to be performed through third-party certification, as it is for audit rights[[3]](#footnote-4).

43. For that purpose, in case of outsourcing of critical or important functions, a firm, applying a risk-based approach, should, using pooled audits, vendor internal audits or third-party certifications where available, at least:

a) …

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

***Article 44:***

Selected components of the exit strategy require firms to “ensure” that certain activities are undertaken by the relevant CSP. While firms can attempt to include obligations on CSPs by way of contract, firms are unlikely to be able to “ensure” that these are met without physical access to the CSP, which is unlikely.

44. In case of outsourcing of critical or important functions, a firm should ~~ensure that it is~~ be able to exit cloud outsourcing arrangements without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with the applicable legal requirements, as well as the confidentiality, integrity and availability of its data. To achieve this, a firm should:

a)…

b)…

c) include an obligation in ~~ensure that~~ the cloud outsourcing written agreement ~~includes an obligation~~ for the CSP to orderly transfer the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy;

d) request confirmation ~~ensure~~ that any data removed or transferred is securely deleted from the systems of the CSP and, where applicable, of any sub-outsourcer ~~(for example, by requesting a written confirmation by the CSP)~~.

***Article 45:***

Sub-article (e) requires the testing of the exit strategy. This is not a standard business requirement and, notwithstanding the fact that CSPs would be unlikely to undertake such an exercise, it is unclear how this could be effectively achieved in practice.

45. When developing the exit plans and solutions referred to in points (a) and (b) above (‘exit strategy’), the firm should consider the following:

a)…

1. ~~e) test the exit strategy, using a risk-based approach;~~

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

Regulated entities may sometimes have challenges in negotiating with third-party service providers of Software-as a-Service or other cloud services where the vendor solution is provided one-to-many and the provider does not want to deviate from its set terms. These challenges tend to arise more with smaller vendors that are not accustomed to providing services to regulated financial services companies. Onsite audit rights can be difficult to negotiate when “onsite” means visiting a server farm that will not yield helpful information as to the actual security of the data. Permitting external personnel to walk through the facility and perform an onsite audit or test could potentially compromise the security of the vendor’s equipment. In addition, limiting the vendor’s ability to subcontract can be challenging where the nature of a technology service involves many back-end providers that do not have logical or physical access to a firm’s data. In this context, firms should be able to rely on vendor internal audits, pooled audits and third-party certifications where traditional audit exercises are either not possible or would only yield limited results.

***Article 52:***

As regulated entities are unable to delegate regulatory compliance, we are unsure why an additional assessment is necessary to ensure whether audits or certification meet regulatory obligations. We understand this also to be a requirement under the EBA Guidelines[[4]](#footnote-5) but importantly, this is only for critical or important functions.

52. ~~In any case~~ For critical or important functions, 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.

***Article 53:***

While we have expressed our reservations on the ability to physically access the premises of a CSP, where firms are required to perform an onsite audit, there should be flexibility to dispense with notice of an inspection if it means that the audit would not be effective, for example, if serious issues at the CSP are suspected.

53. A firm should ensure that, before a planned on-site visit, including by a third party appointed by the firm (for example an auditor), prior notice within a reasonable time period is provided to the CSP, unless an early prior notification is not possible due to an emergency or crisis situation or it would reduce the effectiveness of the visit (for example, serious issues at the CSP are suspected). Such notice should include the location, purpose of the visit and the personnel that will participate to the visit.

***Article 54:***

As the use of cloud services has expanded over the years and become an industry standard for many sectors, not all outsourcing to CSPs should be regarded as technically complex or subject to jurisdictional challenges. We suggest that this article be rephrased so that it is applied only where these factors are prevalent based on a risk-based assessment.

54. Following a risk based assessment, where ~~Considering that~~ cloud solutions present a high level of technical complexity and raise specific jurisdictional challenges, the staff performing the audit – being the internal auditors of the firm or a pool of auditors acting on its behalf – should have the right skills and knowledge to properly assess the relevant cloud solutions and perform effective and relevant audit. This should also apply to the firms’ staff reviewing the certifications or audit reports provided by the CSP.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

No comment.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

***Article 57:***

The requirement to notify ESMA of “planned” outsourcing goes beyond existing reporting requirements as well as those of the EBA Guidelines. The Draft Guidelines should establish a regulatory framework regarding the governance of outsourcing to CSPs but should not introduce regulatory approvals on business decisions. Many of the notification requirements outlined in Article 58 would also be difficult to obtain during the “planning” stage as these would only be available on the conclusion of an agreement. Any obligations to provide pre-outsourcing notification or to obtain approvals would delay a firm’s ability to engage efficiently with the third-party vendors. We strongly suggest that “planned” is deleted.

57. In the case of ~~planned~~ outsourcing of critical or important functions, a firm should notify its competent authority in a timely manner.

<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 comment

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

No comment

<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 comment

<ESMA\_QUESTION\_COGL\_12>

1. [EBA Guidelines on Outsourcing Arrangements 2019](https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements) [↑](#footnote-ref-2)
2. See Article 64 of the EBA Guidelines. [↑](#footnote-ref-3)
3. See Article 49 of the Guidelines. [↑](#footnote-ref-4)
4. See Article 92 of the EBA Guidelines. [↑](#footnote-ref-5)