|  |
| --- |
| 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 | Alternative Investment Management Association (AIMA) |
| Activity | Investment Services |
| Are you representing an association? |  |
| Country/Region | International |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

The Alternative Investment Management Association Limited (AIMA)[[1]](#footnote-2) appreciates the opportunity to submit comments on the European Securities and Markets Authority (ESMA) consultation paper on draft guidelines for outsourcing to cloud service providers.[[2]](#footnote-3)

Cloud outsourcing is increasingly used across the alternative investment industry. With obvious advantages including operational efficiencies and cost-effectiveness, it is unlikely that this trend will slow or reverse in the future. We appreciate, however, that if not properly managed then outsourcing to cloud service providers can also entail challenges in terms of data protection, cyber security issues and concentration risk. Therefore, we support ESMA in its objective to help guide firms on a proportional basis to identify and address potential risks that could arise specifically from cloud outsourcing arrangements, such as selecting a cloud service provider to monitoring outsourced activities and providing for exit strategies.

We previously responded to the European Banking Authority (EBA)’s public consultation on draft guidelines on outsourcing arrangements,[[3]](#footnote-4) where we agreed with the EBA that additional safeguards should be in place when an outsourced activity is critical in nature but maintained that such prudence should not jeapordise the legitimacy and viability of outsourcing arrangements that have proven their worth in helping investors meet their asset allocation requirements. We also previously responded to the EBA’s consultation on draft recommendations on outsourcing to cloud service providers,[[4]](#footnote-5) where we raised concerns regarding immaterial outsourcing, access to business premises, assessing content of certifications or reports, audit options, skills and knowledge verification, right of audit and chain outsourcing.

The final EBA guidelines,[[5]](#footnote-6) which entered into force on 30 September 2019, integrated the EBA’s final recommendations on outsourcing to cloud service providers.[[6]](#footnote-7) We are supportive of the principle of proportionality that the requirements set out in these guidelines are subject to, ensuring that they take into account, in particular, the institution’s size and internal organisation and the nature, scope and complexity of its activities. We are pleased to see that ESMA has also taken into account the principle of proportionality when drafting its new guidelines on outsourcing to cloud service providers.

Overall, we are in broad agreement on the intent of the draft ESMA cloud outsourcing guidelines as a measured approach to proportionally balance risk and complexity, while promoting flexibility to support increased future cloud adoption. We believe that the key to good outsourcing is appropriately managing the associated risks.

In summary, the key points in our response are:

* Investment managers should adopt a risk-based approach to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the cloud service provider;
* the guidelines should differentiate between critical functions and non-critical functions, to take into account the risk underlying the outsourcing of those functions. We agree that the focus should be on the outsourcing of critical functions;
* given the range of different risk models of firms that constitute the AIMA membership, members would welcome additional guidance as to how the pre-outsourcing analysis should be proportionate to the nature, scale and complexity of the function that the firm intends to outsource;
* smaller firms will have reduced negotiating leverage versus larger cloud service providers thus certain guidelines might prove to be unfeasible if outside scope of the agreement;
* relying on the business reputation of the cloud service provider may disadvantage start-up providers who are new to the cloud computing market and potentially discourage innovation and new entrants to the market;
* data centres should be specifically carved out of the references to “premises” and the right of physical access to data centres should be substituted for a right of access to the relevant systems information;
* the adoption of cloud technology may have a mitigating impact on information security risks whereby cloud service providers may have more sophisticated systems to detect and prevent ICT and cyber incidents than local data centre providers or individual regulated entities;
* the testing of exit plans in a practical sense may be an overly burdensome exercise, hindering the take-up of cloud computing. ESMA should clarify that non-practical testing of exit strategies is adequate;
* for smaller firms relying on a third party certification or service provider’s audit because they do not have an in-house technical function, it will be very difficult to assess whether the persons performing the audit “have the right skills and knowledge to properly assess the relevant cloud solutions and perform effective and relevant audit”. Absent a level of self-certification from the suppliers of such services, it will be difficult for people without those skills to judge whether others do have those skills; and
* consideration should be given to how third-party risk-assessment utilities could simplify the assessment process by executing best-practice, standardised evaluations once and making them available to many institutions.

We hope that you find our comments helpful. For further information please contact James Delaney, Director of Asset Management Regulation ([jdelaney@aima.org](mailto:jdelaney@aima.org)).

<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>

We believe that investment managers should adopt a risk-based approach to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the cloud service provider. We were pleased to see that the draft guidelines also advocate for a risk-based approach, for example, when monitoring the performance of activities, the security measures and the adherence to agreed service levels by its cloud service provider.

We agree with the approach taken by ESMA whereby firms complying with these guidelines should take into account the nature, scale and complexity of their business. The proportionality aspect is key. Given the differing sizes of investment managers, establishing a separate outsourcing oversight function will not always be practicable so we support the approach for firms to instead make a senior staff member responsible for overseeing the cloud outsourcing arrangements.

We agree with ESMA that the guidelines should differentiate between critical functions and non-critical functions, to take into account the risk underlying the outsourcing of those functions. We agree that the primary focus should be on the outsourcing of critical or important functions.

We would strongly encourage national competent authorities to factor in the additional resources and time that will be required for firms to comply with these new guidelines. For example, this might include updating an organisation’s digital infrastructure as well as training existing staff or hiring new additional staff.

The suggested approach will place a burden on the cloud service providers as well and ESMA should factor in the amount of involvement the firm will need from the providers. As most will have existing contracts, the tasks that require consultation with the provider may be chargeable and a significant undertaking. They may need to perform the task for new contracts or at renewal of term.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

We note that the draft guidelines propose to require firms to maintain an updated register of information on all its cloud outsourcing arrangements regardless of its materiality status. We believe that this creates an additional burden on outsourcing institutions with little to no benefit and therefore should not be required. We believe that the focus should be on the outsourcing of critical or important functions.

It is our view that a registration requirement of this kind on all cloud outsourcing arrangements, rather than just those of a critical or important nature, would generate a disproportionate burden on outsourcing institutions to no discernible benefit and therefore should not be required.

While it is of course always possible for an outsourced activity to become critical or important, even if it is not so at that given moment, such oversight as expected in the form of a universal central register appears unwarranted. The responsibility would still be with the outsourcing institution to notify its national competent authority when an activity becomes critical or important. This appears a more proportionate approach to the issue at hand here where the primary focus should be on the outsourcing of critical or important functions.

We believe also that it is unnecessary to require a firm to provide a summary of why each outsourced function is or is not considered critical or important. We do not believe that this would be a particularly useful exercise and would suggest instead that firms only need to provide a brief summary for an outsourced function that is deemed to be critical or important.

We would support further clarity on the “appropriate time period” whereby a firm should maintain a record of terminated cloud outsourcing arrangements.

We believe consideration should be given as to whether point 29 section l) ought to also state the outsourced company should perform the same steps (a through k) for the third party (‘sub-outsourcer’) they are using to provide the service. For example, many SaaS providers will build their own software using, for example, an Amazon or Azure data centre.

<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>

Given the range of different risk models of firms that constitute the AIMA membership, members would welcome additional guidance from ESMA as to how 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.

We believe that it may be difficult for some firms to assess risks such as political stability, the security situation and the legal system of the countries where the outsourced functions would be provided and where the outsourced data would be stored. Likewise, it might be challenging for some firms to ensure that the cloud service provider has the business reputation, the skills, the resources and the organisational structure when assessing the suitability of the provider. Also, relying on the business reputation of the cloud service provider may disadvantage start-up providers who are new to the cloud computing market and potentially discourage innovation and new entrants to the market.

We could see some value to firms if ESMA were to provide a list of cloud service providers that are ‘preferred’ or a list of certifications firms should look for (e.g., ISO, ISAE, SOC).

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

We would stress that requiring physical access to where data is stored may make it impossible for investment managers to use public cloud services. We therefore consider that data centres should be specifically carved out of the references to “premises” and the right of physical access to data centres should be substituted for a right of access to the relevant systems information. In other words, seeing racks of blinking lights is of little value but being able to see infrastructure diagrams and setup might be useful in some instances. Increasingly, physical infrastructure is being replaced with software-defined infrastructure so there is nothing to see, or it could be split over multiple locations on shared physical infrastructure.

It would be helpful if the final guidelines were to clarify that the right of access for the supervising authority to information, is done via the outsourcing institution, i.e., the competent authority requests the information from the outsourcing institution who must have the access and pass the information on, rather than direct access to systems of the cloud service provider.

We would query whether the requirement for a firm to “monitor the [provider’s] performance on a regular basis” is in actual fact a realistic requirement for some firms. It might be helpful if further clarity was provided on the expected frequency of a “regular basis”, e.g. on an annual basis.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

We agree with the suggested approach that firms should adopt a risk-based approach to information security considerations in the case of outsourcing to cloud service providers.

We think it might be helpful to include in this section a clear statement on shared responsibility. Firms need to make sure they clearly understand the separation of what they are responsible for and what the cloud service provider is responsible for when it comes to information security requirements.

We would also note that the adoption of cloud technology may have a mitigating impact on information security risks whereby cloud service providers may be more aware of cyber security issues and have more sophisticated systems to detect and prevent ICT and cyber incidents than local data centre providers or individual regulated entities.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

We agree that in the case of outsourcing of critical or important functions, a firm should ensure that it is 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.

We would question the ability of firms to fully test the exit strategy as certain elements of the strategy, such as the orderly transfer of the outsourced function and all the related data from the cloud service provider and any sub-outsourcer to another provider indicated by the firm, might be challenging in reality. We believe that testing exit plans in a practical sense may be an overly burdensome exercise, hindering the take-up of cloud computing. We believe that ESMA should clarify that non-practical testing of exit strategies is adequate.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

We support the suggested approach that a firm should ensure that the outsourcing written agreement does not limit the firm’s effective exercise of the access and audit rights as well as its oversight options on the cloud service provider. We also agree that a firm should take into consideration whether the outsourcing is related to a critical or important function, as well as the nature and extent of the risks and impact arising from the cloud outsourcing arrangement on the firm.

For smaller firms relying on a third party certification or service provider’s audit because they do not have an in-house technical function, it will be very difficult to assess whether the persons performing the audit “have the right skills and knowledge to properly assess the relevant cloud solutions and perform effective and relevant audit”. Absent a level of self-certification from the suppliers of such services, it will be difficult for people without those skills to judge whether others do have those skills.

We believe that consideration should be given to how third-party risk-assessment utilities could simplify the assessment process by executing best-practice, standardised evaluations once and making them available to many institutions.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

We believe that it might be difficult in practice for a firm to “ensure that the cloud service provider appropriately oversees the sub-outsourcer”. There will need to be an element of reliance and trust on the part of the firm that the cloud service provider is carrying out the required monitoring of the sub-outsourcer, especially for smaller firms with fewer resources.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

We agree with ESMA that appropriate notification requirements should be followed when an outsourced activity is critical in nature. However, we would question the benefit of the requirement for a firm’s written notification to include where the cloud service provider as well as any sub-outsourcer will store and process the data. This focus on data locality is seen as problematic, especially given that, currently and even more in the future, it is likely that technology will continue to evolve in a direction where physical location of data will become less and less clear.

<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>

We are supportive of the approach that competent authorities should focus on the arrangements that relate to the outsourcing of critical or important functions and are also supportive that any assessment is carried out on a risk-based approach.

We believe that removing any existing uncertainty regarding supervisory authorities’ practices will help increase the adoption of cloud computing. A consistent supervisory approach on cloud outsourcing would allow for economies of scale for firms and cloud service providers with regards to compliance costs.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

The greatest risk is concentration if many firms use the cloud for Infrastructure as a Service. There is a great overhead and cost for firms to have full cloud supplier diversity. It could well be the case that much of the financial industry is on one provider in the future. Any large outage of that provider could ripple through the industry causing massive operational loss. It is not easy for firms to code their infrastructure environment for more than one cloud provider, as they would essentially double their effort and thereby potentially lose foreseen cost efficiencies.

We would again suggest referencing a few certifications that cloud service providers will hold as this could assist firms by simplifying the analysis they might need to perform.

Overall, we are in broad agreement on the intent of the draft ESMA cloud outsourcing guidelines as a measured approach to proportionally balance risk and complexity, while promoting flexibility to support increased future cloud adoption. We believe that the key to good outsourcing is appropriately managing the associated risks.

We would also like to add that we have published relevant sound practices guides for the alternative investment industry to aid investment managers when outsourcing functions. [AIMA’s Guide to Sound Practices for Outsourcing by Investment Managers](https://www.aima.org/sound-practices/guides-to-sound-practices.html) and [AIMA’s Guide to Sound Practices for Cyber Security](https://www.aima.org/uploads/assets/d44af1dc-6dab-4714-94f3708982c7f550/AIMA-Guide-to-Sound-Practices-for-Cyber-SecurityExecutive-Summary-November-2019.pdf) cover agreements relating to cloud computing. We note that the investment manager will need to take a risk-based approach to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the cloud service.

<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>

We do not have detailed information on the direct costs linked to the update/review of the existing procedural and organisational arrangements, direct initial and ongoing IT costs, or the direct relevant organisational and HR costs linked to the implementation of these guidelines, however we would strongly encourage competent authorities to factor in the additional resources and time that will likely be required for firms to comply with these new guidelines. For example, this might include updating an organisation’s digital infrastructure as well as training existing staff or hiring new additional staff.

<ESMA\_QUESTION\_COGL\_12>

1. AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with around 2,000 corporate members in over 60 countries. AIMA’s fund manager members collectively manage more than $2 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA’s website, [www.aima.org](http://www.aima.org). [↑](#footnote-ref-2)
2. <https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines>. [↑](#footnote-ref-3)
3. <https://eba.europa.eu/eba-consults-on-guidelines-on-outsourcing>. [↑](#footnote-ref-4)
4. <https://eba.europa.eu/sites/default/documents/files/documents/10180/1848359/c1005743-567e-40fc-a995-d05fb93df5d1/Draft%20Recommendation%20on%20outsourcing%20to%20Cloud%20Service%20%20(EBA-CP-2017-06).pdf> [↑](#footnote-ref-5)
5. <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf> [↑](#footnote-ref-6)
6. <https://eba.europa.eu/sites/default/documents/files/documents/10180/2170121/5fa5cdde-3219-4e95-946d-0c0d05494362/Final%20draft%20Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03).pdf> [↑](#footnote-ref-7)