167 Fleet Street, London EC4A 2EA, UK
+44 (0)20 7822 8380
info@aima.org

aima.org

European Banking Authority
Floor 46
One Canada Square
Canary Wharf
London E14 5AA

Submitted via link on consultation page

15 August 2017

Response to Consultation on Draft Recommendations on Outsourcing to Cloud Service Providers under Article 16 of Regulation (EU) No 1093/2010

The Alternative Investment Management Association (AIMA)[1] thanks you for this opportunity to respond to the European Banking Authority's (EBA) consultation paper on draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010 (the 'Consultation Paper'). We understand that these recommendations, if and when adopted, would be directed to national competent authorities, credit institutions and investment firms as defined in the Capital Requirements Regulation (Regulation (EU) No 575/2013) ('CRR'). Although the CRR definition of investment firm captures a relatively small percentage of AIMA member firms, we are responding from the perspective of our wider membership as well. Whatever recommendations EBA finally adopts in this regard are likely to inform any similar work undertaken by the European Securities and Markets Authority with regard to alternative investment fund managers under AIFMD, UCITS management companies under the UCITS Directive and non-CRR investment firms under MiFID.

In respect of the specific questions posed in the Consultation Paper, we believe the recommendations are clear (subject to the points raised below), further details would likely be unhelpful and there are no additional areas that we think should be covered.

[1] AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with more than 1,800 corporate members in over 50 countries. AIMA's fund manager members collectively manage more than $1.8 trillion in 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 proactively communicates with the media and the general public to increase awareness around the value of the industry. AIMA set up the Alternative Credit Council, or ACC, to help firms focused in the private credit and direct lending space. The ACC currently represents over 80 members that manage $300 billion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) - 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.

We note that the draft recommendations are not supposed to be exhaustive, but we do consider that some of the draft recommendations could be made clearer and less prescriptive. In particular, we have a few concerns with the proposed recommendations as currently drafted that we would like to see addressed in the final version which relate to the following:

- **Business continuity plan suitability:** In paragraph 3(a), the recommendation that competent authorities may ask outsourcing institutions for additional information, including the outsourcing institution's analysis of "whether the cloud service provider has a business continuity plan that is suitable for the service provided to the outsourcing institution" would require each outsourcing institution to assess the business continuity plan of the cloud service provider. Even if the assessment requirement is narrowly drawn to the services being provided, the requirement to represent to the competent authority that the business continuity plan "is suitable" presents multiple questions. What would be the consequence of a representation that a selected cloud service provider did not have a "suitable" business continuity plan? What happens if one outsourcing institution concludes it is suitable but another outsourcing institution does not? Would an outsourcing institution face a regulatory or other liability if it represents that the plan is suitable but it later turns out that the plan fails? We would recommend deleting paragraph 3(a);

- **Immaterial outsourcing:** Paragraph 4.3 of the CEBS Guidelines on Outsourcing (14 Dec. 2006) ('CEBS Guidelines') states that "[a]n outsourcing institution should take particular care when outsourcing material activities. The outsourcing institution should adequately inform its supervisory authority about this type of outsourcing." Paragraph 5 of the CEBS Guidelines goes on to say "[t]here should be no restrictions on the outsourcing of non-material activities of an outsourcing institution" and "In such cases the outsourcing institution does not need to adequately inform its supervisory authority." We believe these provisions struck the right balance from a cost benefit point of view. We note, however, that the Consultation Paper proposes to reset that balance fundamentally by requiring all outsourcing activities to be recorded in the register regardless of its materiality status. We believe that this extension creates an additional burden on outsourcing institutions with no benefit and therefore should not be required. If outsourcing institutions are ultimately required to add immaterial outsourcing arrangements to their outsourcing registers as recommended in paragraph 4, there should be a transition period for compliance since that level of register recording has not previously been required;

- **Access to business premises:** Requiring physical access to where data is stored may make it impossible for asset management firms to use public cloud services. We therefore consider that data centres should be specifically carved out of the references to "business premises" and "operations centers" in paragraphs 6(a), 10(a), 14(a) and 14(b) or 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 use but being able to see infrastructure diagrams and setup might be useful. Increasingly physical infrastructure is being replaced with Software-defined Infrastructure so there is nothing to actually see – or it could be split over multiple locations on shared physical infrastructure;

- **Assessing content of certifications or reports "continuously":** The recommendation in paragraph 8(b)ii requires the outsourcing institution to assess "the content of the certifications or audit reports continuously" in particular to ensure that key controls are still covered in future versions. We are not sure what is meant by continuously in light of the further wording about

ensuring that controls are still covered in future versions. We believe the ambiguity could be resolved without changing what appears to be intended simply by removing the word "continuously" from the recommendation;

- **Audit options:** In paragraph 8(b)v, there is a requirement that to use the third party certification method and cloud service provider pays methods, the outsourcing institution has to have the contractual right to request the expansion of scope of the certifications and the "number and frequency of such requests for scope modification should be **reasonable**, and **legitimate** from a risk management perspective." (emphasis added) However, "reasonable" and "legitimate" are subjective concepts with no definition and which the recommendation seems to require be left to the outsourcing institution's unfettered judgment. It is extremely unlikely that a cloud service provider would agree to such terms, which will make the third party certification method and cloud service provider pays models unworkable in practice. We recommend removing the last sentence of paragraph 8(b)v;

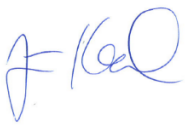
- **Skills and knowledge verification:** For smaller firms relying on a third party certification or service provider's audit because they do not have an in-house technical function, it will be very difficult to assess whether the persons performing the audit "have acquired the rights skills and knowledge to perform effective and relevant and/or assessments of cloud solutions. 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. Moreover, it is not realistic to require all of the users of a third party certification or audit report to have to have access to the individuals who performed the audit in order to each separately assess the skills and knowledge of those individuals;

- **Right of audit:** Paragraph 10(b) recommends that the written outsourcing agreement contain an undertaking granting the competent authority supervising the outsourcing institution "unrestricted rights of inspection and auditing of the outsourcing institution's data". It would be helpful if the final recommendations 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; and

- **Chain outsourcing:** It would be helpful if it was made clear that the chain outsourcing recommendations apply only to material outsourcing arrangements, e.g., the outsourcing institution should not have to audit who performs basic building maintenance.

We hope you have found these comments to be helpful. We would be happy to answer any questions you may have in relation to this submission.

Yours sincerely,



Jiří Król
Deputy Chief Executive Officer
Global Head of Government Affairs