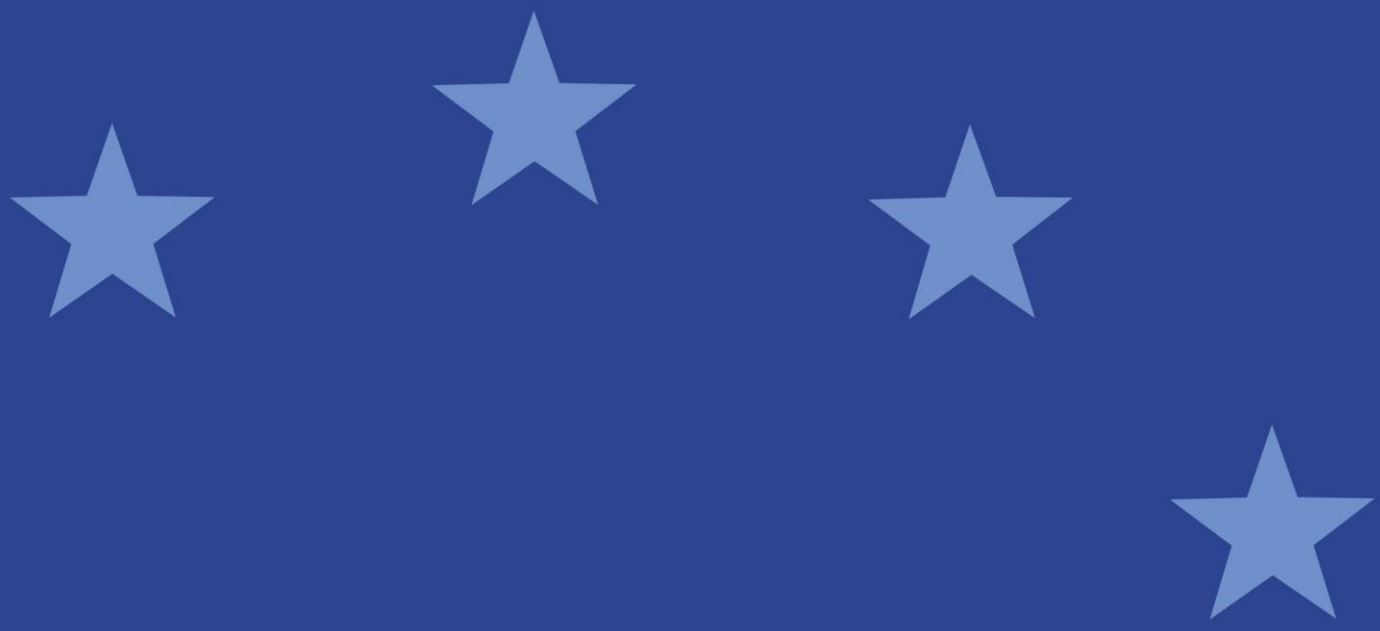
esma European Securities and Markets Authority

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	Finance Denmark
Activity	Other Financial service providers
Are you representing an association?	☒
Country/Region	Denmark

Introduction

Please make your introductory comments below, if any

<ESMA_COMMENT_COGL_1>

Finance Denmark welcomes the opportunity to respond to ESMAs consultation paper on guidelines on outsourcing to cloud service providers (ESMA GL). Finance Denmark finds it positive that ESMA provides guidelines in this area, and that ESMA has considered the EBA Outsourcing Guidelines (EBA GL) in the drafting of the ESMA GL. However, we see a risk in having differentiated guidelines where firms are regulated by both EBA and ESMA as this could result in excessive administrative burdens and futher complicate the implementation of a complex regulation. A consistent supervisory framework under both ESMA GL and EBA GL is preferable.

Therefore we encourage a further alignment with the EBA GL in order to ensure that firms, who are regulated by both EBA and ESMA, operate under a streamlined supervisory framework, especially in regards to

- Being more clear and specific on what is required as in the EBA GL in order to ensure a harmonised framework and a consistent implementation and application of the ESMA GL across the financial sector;

- Ensure that the definition and scope of critical and important outsourcing is alignet with EBA GL in order to avoid interpretation differences;

- Ensure that the ESMA GL also include which functions that are not considered outsourcing as in the EBA GL and that the differences in scope of the EBA GL and ESMA GL is taken into consideration in this respect;

- Provide more guidance on how the guidelines apply in case of intra-group outsourcing of IT functions, i.e. from a subsidiary to a parent company or an affiliate company.

This view is reflected in our comments below.
<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>
There is a general obligation for firms to define and keep a cloud outsourcing strategy up to date in the ESMA GL paragraph 25. There is very little detail about what should be included within such a cloud outsourcing strategy compared to the EBA GL paragraph 41, 42, 43 and 44. We suggest ESMA to include more guidance on what should be covered in such a cloud outsourcing strategy, including that the outsourcing strategy should differentiate between outsourcing arrangements as set forth in the EBA GL, paragraph 43. Further, in respect of the ESMA GL, paragraph 26, we suggest that it is elaborated in the ESMA GL if small and less complex firms also need to establish an outsourcing oversight function or designate a senior staff member.

The ESMA GL paragraph 28 states that firms must provide a brief summary of the reasons why the outsourced function is or is not considered critical or important. The number of foreseen non-critical functions is high and therefore explaining why each is non-critical would result in a high degree of work which undermines the principle of proportionality and a risk-based approach.

We suggest instead that a firm should have to clarify its criteria for materiality and process for determining that materiality once, allowing the regulator to request further info in the event that a specific function requires further detail. This would also be better aligned with the EBA GL, which state in paragraph 54 that an explanation is required for why an outsourced function is considered critical or important, rather than why it is not.

Furthermore, we encourage ESMA to amend the naming convention for this document from “cloud outsourcing strategy” to “cloud outsourcing policy” to better align the terminology used in the EBA GL (i.e. “outsourcing policy”).
<ESMA_QUESTION_COGL_1>

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

<ESMA_QUESTION_COGL_2>

The list for what should be recorded in the register for critical or important cloud outsourcing arrangements is very detailed in the ESMA GL paragraph 29 but there is little guidance on what should be included in the register for non-critical or important cloud outsourcing arrangements in the ESMA GL paragraph 30. We encourage ESMA to give more guideance on what should be included in the register for non-critical or important cloud outsourcing-arrangements, which would also align the guidelines to paragraph 54 of the EBA GL.

It may otherwise leave room for NCAs to adopt an approach which deviates from those set out by the EBA which could result in an inconsistent register regime between non- critical/important cloud outsourcing under the approach of the EBA GL and ESMA GL for those dual regulated firms.
<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>
If concentration risk is to be assessed within the sector, we believe that this should be done directly by authorities. For risks of this nature, authorities (e.g. supervisory bodies) are well positioned to have oversight at an industry level, as compared to firms individually. We believe, however, that any such assessment should not restrict the choice of outsourcing arrangements or providers available to firms. The focus should be on reducing the risks arising from concentration rather than reducing concentration itself which we believe would be difficult and require undesirable sacrifices to security, efficiency and innovation.

In terms of an assessment of possible concentration within the firm caused by multiple cloud outsourcing arrangements with the same CSP, firms should be able to undertake this as an internal assessment, based on risk appetite, and not be mandated to assess this on stipulated metrics that are set in regulatory guidance.

Any such metrics would struggle to account for the range of business models and outsourcing arrangements across the industry.
<ESMA_QUESTION_COGL_3>

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

<ESMA_QUESTION_COGL_4>
The scope of the contractual requirements under the ESMA GL paragraph 41 should be extended. For example, the contractual requirement under the ESMA GL paragraph 41 (f) should be extended to require the specification of the country from which the services will be provided as is required under the EBA GL paragraph 75(f). Further, the auditing requirement under the ESMA GL paragraph 41(n) should be “unrestricted” as is required under the EBA GL paragraph 75(p).

In addition, we recommend that a number of additional contractual requirements are included. This should include: (i) an obligation for cloud service providers to cooperate with competent authorities as is the case under the EBA GL paragraph

75(n) and (ii) and specific requirements rearding termination rights of the firm as is the case under EBA GL paragraph 75(q).
<ESMA_QUESTION_COGL_4>

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

<ESMA_QUESTION_COGL_5>
We encourage ESMA to provide further guidance on what should be included within the scope of the business continuity and disaster recovery plans under the ESMA GL paragraph 43(f), in line with the guidance in the EBA GL paragraph 48 and 49.

We suggest that the ESMA GL in line with the EBA GL, paragraph 106. includes that an exit strategy should be in place, and further include the requirements to such exit strategy (as in the EBA GL, paragraph 106.) Further, we suggest that the ESMA GL includes an elaboration on the differences between an exit strategy and an exit plan.
<ESMA_QUESTION_COGL_5>

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

<ESMA_QUESTION_COGL_6>
TYPE YOUR TEXT HERE
<ESMA_QUESTION_COGL_6>

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

<ESMA_QUESTION_COGL_7>
We encourage ESMA to expand the scope of such access and audit rights against cloud service providers. Specifically, we recommend expanding the scope to allow firms, competent authorities and their representatives to be provided full access and unrestricted rights of inspection as is the case under the EBA GL paragraph 87.

We suggest including the following statement in the ESMA GL paragraph 53 '*or would lead to a situation where the audit would no longer be effective*'.
<ESMA_QUESTION_COGL_7>

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

<ESMA_QUESTION_COGL_8>
We suggest that the following additional restrictions regarding sub-outsourcing are included: (i) a requirement that the cloud service provider obtain specific or general written authorisation from the firm before sub-outsourcing data as is the case under the EBA GL paragraph 78(d), (ii) a requirement that the cloud service provider ensure that subcontractors comply with applicable laws, regulatory requirements and contractual obligations as is the case under the EBA GL paragraph 79, and (iii) a requirement that cloud service providers ensure that subcontractors grant firms and

competent authorities the same contractual rights of access to sub-outsourcers as the cloud service provider as is the case under the EBA GL paragraph 79. Further, we suggest that it – as in the EBA GL, paragraph 80 – is stated in the ESMA GL, paragraph 56, that overseeing the sub-outsourcer should be in line with the policy defined by the firm.
<ESMA_QUESTION_COGL_8>

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

<ESMA_QUESTION_COGL_9>
We recognise the necessity of providing adequate notification to authorities,but pre-approval requirements are a barrier to financial institutions in attempting to keep up with innovation and competition from other sectors. We encourage ESMA to aligne the notification procedure to the EBA GL thereby clarifying that there is not a pre-approval procedure in the ESMA GL.

If a non-critical or important outsourcing arrangements later becomes a critical or important outsourcing arrangement through, for example, a change in scope or deliveries, there is no express requirement for the firm to notify a competent authority of such change as is the case under the EBA GL paragraph 58. We suggest such a notification obligation requirement is included to ensure adequate oversight of cloud outsourcing arrangements in order to ensure clear guidance on this point.
<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>
We find that the guidance to supervisory authorities on the supervision of cloud outsourcing arrangements is not sufficiently detailed. The focus of the requirements is limited to: (a) a requirement for competent authorities to focus their assessments on critical or important cloud outsourcing arrangements and those arrangements that are outside the EU, (b) some brief details about what should be assessed by the competent authorities, and (c) an obligation to monitor firms where risks are identified.

The lack of detailed guidance may give rise to different approaches to the supervision of cloud outsourcing arrangements causing a lack supervisory convergence between member states. For groups operating in different countries this may give rise to unnessasary administrative burdens of having to comply with local supervisory requirements in various countries.
<ESMA_QUESTION_COGL_10>

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

<ESMA_QUESTION_COGL_11>

Reference	Title	Assessment
3.1 Scope	N/A	We suggest that it is clarified whether the ESMA GL apply to UCITS that are not managed by a UCITS management company and whether the guidelines apply to both outsourcing done by a UCITS management on behalf of the UCITS managed by it and outsourcing done in connection to the operation of the UCITS management company as such.
3.1 Scope	"Who?"	The ESMA GL apply to depositaries of AIFs and UCITS. The AIFMD and the UCITS Directive sets out strict restrictions under which depositaries are allowed to delegate the safekeeping of assets of AIF and UCITS respectively, whereas the delegation of depositary functions is not permitted. However, as is also clarified in the recitals of the AIFMD and the UCITS Directive as well as ESMA's Q&A on the application of the AIFMD and the UCITS Directive respectively, delegation of supporting tasks that are linked to its depositary tasks, such as administrative or technical functions, is not subject to the specific limitations and requirements set out in the AIFMD and the UCITS Directive. As the difference between "delegation" (as this term is used in the AIFMD and UCITS Directive) and "outsourcing" (as this term is used in these draft guidelines) is not quite clear, we recommend that it is specified in which situations the depositary is able to outsource to a cloud service provider (without being non-compliant with the AIFMD and UCITS Directive rules referred to above) – and thereby subject to the ESMA GL.
3.1 Scope	N/A	The ESMA GL should contain guidance on how the guidelines apply in case of intra-group outsourcing of IT functions, i.e. from a subsidiary to a parent company or an affiliate company.
3.2 Legislative references, abbreviations and definitions – Definitions	"critical or important function"	The definition of "critical or important outsourcing" reflects the main considerations for identifying a critical or important outsourcing under the EBA GL paragraph 4). However, there are a number of additional considerations that are included in the EBA GL to 'flesh out' to identify a critical or important

		outsourcing cf. EBA GL paragraph 29(b), 29(c), 30, 31. We suggest expanding the scope of what should be considered when conducting an assessment of a critical or important cloud outsourcing arrangement, to ensure firms have sufficient information to make this assessment. The ESMA GL should further include a list of functions which are not considered outsourcing as in the EBA GL, paragraph 28. In this respect, the differences in scope of the EBA GL and ESMA GL should be taken into consideration. We also encourage that further consideration is given to the additional input included within the EBA GL cf. EBA GL paragraph 29(b), 29(c), 30, 31.
3.2 Legislative references, abbreviations and definitions – Definitions	Private Cloud	The ESMA GL defines private cloud with reference to a model where “cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer”. This contrasts with the EBA GL definition (paragraph 12) which notes that private cloud is “cloud infrastructure available for the exclusive use by a single institution or payment institution”. The EBA GL definition is preferable because it leaves open the possibility that the cloud infrastructure can be owned and operated entirely by the consuming firm whereas the term customer implies a third-party relationship. The use of ‘customer’ also creates confusion because it does not acknowledge the range of possibilities within the private cloud deployment model. The inclusion of customer also leaves it open for NCAs to implement their own interpretation of the term and could lead to the need for firms to document more granular detail on their private cloud arrangements. In addition, ‘control’ is also an ambiguous term in this context because, as with ‘consumer’, it covers a range of possible practices depending on the nature of a firm’s private cloud deployment.
3.4 Compliance and reporting obligations –	Reporting obligations	It states that there is no requirement for firms to report on whether they are compliant with the ESMA GL.

status of the guidelines - §24		It is unclear whether “these guidelines” refers to the ESMA Draft Guidelines or the final draft of the guidelines (presumably the prior), as there are specific reporting obligations listed under the ESMA GL paragraph 8. We recommend that this is clarified.

<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>
Based on a high-level assessment on the experience from implementing the EBA GL, the implementation and on-going compliance is expected to be burdensome and a strain on resources especially in the fund management companies and smaller firms.
<ESMA_QUESTION_COGL_12>