|  |
| --- |
| 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. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. 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 | Shared Assessments Program |
| Activity | Non-financial counterparty |
| Are you representing an association? |  |
| Country/Region | Other |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

**Date:** 28 August 2020

**To: Submitted through Online Portal** [www.esma.europa.eu](http://www.esma.europa.eu/)

**From:** Robin Slade, EVP & COO,The Shared Assessments Program robin@santa-fe-group.com

(630) 815-4420

**RE: The Shared Assessments Program Input – Consultations**

**Consultation Paper: Draft Guidelines on Outsourcing to Cloud Service Providers**

The Shared Assessments Program appreciates the opportunity to submit comments to the European Securities and Markets Authority on this consultation paper.

For context, the Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops tools, and conducts pacesetting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. More information on Shared Assessments is available at: [http://www.sharedassessments.org.](http://www.sharedassessments.org/)

We have two general comments regarding the guidelines as a whole:

1. This set of guidelines has a narrow focus on the CSP’s controls and the outsourcer’s requirements for monitoring those controls. The guidance should be expanded to ensure that responsibilities are addressed around security, privacy, change management, continuity, and other configuration controls for which the outsourcer is directly accountable. This general comment is brought forward throughout our responses to the guidelines in context of individual guideline responses.

1. Ideally, these guidelines should be jurisdiction-agnostic to match the global nature of the internet and CSPs.

On behalf of the Shared Assessments Program and its members, thank you for considering the following response regarding ESMA’s Consultation Paper: Draft Guidelines on Outsourcing to Cloud Service Providers.

<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>

**Response and Rationale:** While the suggested documentation requirements will help to strengthen the risk posture of EU firms and supports Privacy by Design by promoting data outflow tracing for the provider’s data processing locations, for firms operating outside the EU this approach may be more problematic due to the granular nature of the approach.

While CSPs may require additional controls, controls should be standardized to span all outsourcing arrangements. Several components included in the guidelines are not CSP-specific controls. Rather, they are controls that should be standardized and applied enterprise wide. For example, 3.5.26, “clearly assign responsibilities” and “establish outsourcing oversight function” should be present in any outsourcing scope of work and vendor management program; and Section 3.5.26.b “allocation of sufficient resources for compliance” should be part of an MSA or a data privacy & security addendum (DPSA) regardless of whether a CSP is involved.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

**Response and Rationale:** The approach is very granular. For instance, with reference to data localization, the need exists to isolate data due to lack of certainty that the data will be transmitted within EU guidelines. This set of guidelines accelerates the need for a localization process without providing hygiene guidelines or requirements to meet that need.

The intended impact on firms that are accustomed to utilizing and/or transmitting data more broadly than these guidelines allow is unclear. With respect to section 3.5.27, to “monitor on a risk-based approach performance of CSP activities, security measures and adherence,” this is unachievable. While performance can be governed by contract, compliance at the CSP level for data transmission tracking cannot be monitored effectively by the outsourcer. In addition, section 3.5.27 requires clarity to define the “performance of activities” as it is difficult to conduct ongoing monitoring for which the CSP is responsible because of commonly accepted contractual restrictions.

Re: Section 3.5.29.j. The documentation requirements are not adequate to track the type of monitoring required by the outsourcer or the CSP. The guideline needs to focus on monitoring the outsourcer’s controls where it interfaces with the CSP’s environment.

Re: Section 3.5.28 & 29. There is no specificity of data field requirements (file format, naming conventions, field sizes/types, etc.) for maintaining an updated register of all CSP arrangements AND what the register should include. We recommend that these guidelines mirror the EBA Outsourcing Guidelines for register requirements, which include: *Section 11. Documentation Requirements 56. Institutions and payment institutions should, upon request, make available to the competent authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point (d) of paragraph 54 of these guidelines (e.g. all IT outsourcing arrangements). Institutions and payment institutions should provide this information in a processable electronic form (e.g. a commonly used database format, comma separated values).* While the need for the register is clear, aspects of information required within these guidelines may not be achievable.

While the register is essential for regulators, as it allows competent authorities to examine information they cannot see in other settings, VPNs and private tunnels can mask or otherwise alter privacy-related data sets (e.g. IP, PII, email addresses, etc.). A unified nomenclature for register formatting would be useful for both outsourcers and competent authorities. A sample would assist outsourcers in meeting the guidelines.

<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>

**Response and Rationale:** For some sectors, such as financial services, the suggested approach for evaluating proportionality is natural. For other industries, it may be less applicable/feasible. Differences may exist between firms that operate in the EU/UK and/or cross jurisdictionally, rather than US-based firms as to what can be achieved.

Re: Section 33.a.v. Portability needs to be considered at an entire service level, not just data.

Re: Section 33.a.vii. The requirement for a centralized means of gauging concentration risk where CSPs are used by multiple units would help outsourcers to recognize the risk is valuable as a tool for better understanding the tension between cost benefits of multiple licensing arrangements and concentration risk. The need for resilience would mandate that firms seek a more distributed use of CSPs, which is difficult for firms to achieve in a market with limited providers.

Re: Section 35. This guideline assumes that other due diligence mechanisms are going to be put into place. The quality of the assessor and relevance of the findings are also factors that may impact due diligence. Artifacts that are related to the CSP reports and certifications are unlikely to be available to the outsourcer. The need for further validation is made clearer in Guideline 6.52. which states that an outsourcer may not rely solely on these reports and certifications. Guideline 35 should mirror Guideline 6.52 to make clear that additional validation is required.

Re: Section 38. The use of the terminology “a risk-based approach” surrounding important services should specify what type of due diligence is required. Also, the use of the term “riskbased approach” is not well defined, i.e. the cadence of re-assessments is not well defined and is not unique to CSPs.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

**Response and Rationale:** Overall, key challenges exist in the CSP ecosystem where most CSP arrangements are “one size fits all”, including access/audit rights, subcontracting notification and/or approval, and monitoring and performance data reporting. In existing relationships, timely contract changes (by the date mandated by the guidelines) may not be possible where changes to guidelines have not been contractually bound.

Re: Section 41.e. Clear definitions are lacking. There is a lack of specificity regarding what terms mean (SLA, regular, monitor, timing, reasonable, etc.). A glossary that includes these terms would be appropriate.

Re: Section. 41.h. The definitions of “regular” and “monitor performance” are not clear. If monitoring requires onsite access, which is dictated elsewhere in the guidelines, that would be appropriate to define in the requirement for monitoring. The right to monitor in any effective manner will be greatly restricted for the vast majority of CSP clients.

Re: Section 41.n. Today, most CSPs will not permit access to secured sites, because they believe that doing so would compromise their security. Given the sensitive nature of the assets that CSPs manage, some form of rationality and process assurance would be needed in contract clauses that cover evaluation and access rights. A positive effect of this guideline could be that it may prod other jurisdictions to follow suit, which would encourage providers to meet this worthwhile requirement outside the EU and help outsourcers to more reliably monitor their CSPs.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

**Response and Rationale:** The approach would benefit from a less prescriptive, more comprehensive approach to accommodate changing standards and rapidly evolving technology and threats. For example, requirements around change controls could be added:

Re: Section 43.c. With reference to horizon scanning and changes in technology the need to upgrade cryptography and encryption technologies that change over time.

Re: Section 43.e. Considering the importance of timely communication between outsourcer and CSP to maintain control compatibility and appropriateness.

Re: Section 42. The monitoring requirement regarding data location may not be achievable, if it requires onsite monitoring or the data cannot be managed in a manner that allows for data location (which can be impacted by VPNs; there will be limited opportunity for an organisation to add its own, or tailor the existing, information security controls applied by the CSP; and other factors that impact data tracking/identification tools).

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

**Response and Rationale:** We agree with the suggested approach overall. However, the guideline lacks specificity. See sections below for details.

Re: Section 44.a and e. Exit plans cannot be effectively “tested” (e.g., while data destruction certificates can be obtained, there is no effective way to test that the data has in fact been removed/destroyed). It may be more useful to use the term “periodic validation” of the exit strategy (e.g., has proof of concept been exercised to validate that the planned backup vendor is still reasonably viable/available, are parallel processes in place and viable, etc.).

Re: Section 46. This guidance would benefit from requiring that trigger events are defined and included in contract terms (agreements); as well as the requirements (processes, etc.) that will take place during exit/termination; and that – as other authorities require – mechanics must be in place when a vendor is terminated that the outsourcer has demonstrated and documented HOW the exit will be accomplished “*without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with the applicable legal requirements* (EBA Outsourcing Guidelines, Section 14.107, 2019)”.

Re: Section 44.d. Reliance must not be made on the CSP to delete or remove data; this is the responsibility of the firm and, to be effective, the ability to securely delete data MUST be built into the architecture of the solution.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

**Response and Rationale:** No, we do not agree with this approach. Specifically:

Re: Section 47. Given the restrictions for audit and access are virtually unachievable in most CSP settings, the use of a format – such as that applied by the U.S. Federal Financial Institution Examination Council (FFIEC) – where the competent authority examines and provides assurance on systemically important third parties. This type of regulatory examination is necessitated by how the industry model has evolved, where the CSP market is so constrained to a small number of providers.

Re: Section 51.g. Onsite audits are not feasible in the current market. Audit frequencies are not specified, and continuous monitoring is absent from the audit requirements.

Re: Section 53. Please define the criteria that constitute an onsite visit.

Re: Section 51.f and g. It is highly unlikely that a CSP will allow the expansion of audit scope and permit onsite audits. It is equally implausible to obtain access and audit rights in the Nth party contract where Nth party contracts are already in place.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

**Response and Rationale:**

Re: Section 55.d. While we agree with the guideline in principle, it may be difficult to implement. See 55.e.

Re: Section 55.e. It may not be practical (dependent on the scope of the change) to permit clients to object to outsourcing changes. CSPs should be required to supply key evidence (SOCs, ISO certifications, IT security reviews, etc.). Where contracts are already in place ahead of the guideline being implemented, this may be difficult to achieve. In our members’ experience, the term “sub-outsourcing” has been challenged by CSPs. Therefore, a precise definition of the term in the context of CSPs would be useful.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

**Response and Rationale:** In theory, we agree. However, the guideline would benefit from clearer definitions, such as what is “timely”. A glossary of terms would be appropriate.

Re: Section 58.i. What type of audit/assessment and proportionality relative to the service/criticality could be added to this guideline.

<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>

**Response and Rationale:** In principle, the suggested approach is valid. The ability to act on this approach is dependent on the ability of the outsourcer and CSP to provide a format that is unified for use by the competent authorities. The response time and communication requirements between outsourcers and competent authorities could be defined.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

**Response and Rationale:** Our constituencies encourage harmonization of global regulatory requirements.

<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>

**Response and Rationale:** For an organisation to examine their cost burden, the guidelines would require at minimum the resources to conduct the following tasks: (1) pre-onboarding review of vendor and services; (2) contract review regarding any controls changes needed over time; (3) ongoing monitoring of criticality and other impacts to the outsourcer; (4) service architecture review for each service migrated to CSP; (5) ongoing architectural review where notification or approval of CSP changes cannot be assured.

This level of oversight and supervision would require an additional cost burden to many firms, especially those that lack the people and tools to carry out the requirements of these guidelines. These guidelines assume a set of resources and processes for Cloud management, including CSP monitoring, that may not be present today. Most firms may have to upskill and use new/adapted tools to govern and monitor CSPs. This would be a considerable additional burden for firms that do not already meet this requirement to reach the level of assurance needed to meet these guidelines.

For those with existing due diligence processes that meet the guidelines, they should not cause significant additional resources and expenditures.

Additionally, if the outsourcer is monitoring its own activities in the cloud, configuration management with continuous monitoring capabilities would be required for the outsourcer’s to perform that monitoring.

<ESMA\_QUESTION\_COGL\_12>