|  |
| --- |
| 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 | BNPPF |
| Activity | Banking sector |
| Are you representing an association? |  |
| Country/Region | Belgium |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

Responses provided by BNPPF

<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>

No remarks/ we agree

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

**No, we do not agree.**

**Rule 29h & 29l -** From a Data Protection point of view, it could be insufficient to only monitor where data may be stored and processed. It should probably be useful to also monitor from where data can be **accessed.**

<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>

No, we do not agree:

**Rule 31** - We consider that "assessing any conflict of interest" is to broad and open to interpretation. Some guidance could help.

**Rule 32** - It is stated that the pre-outsourcing analysis and due diligence should be proportionate to the criticality of the functions the CSP will support. But, from a cyber security point of view, this is somewhere irrelevant. Even a CSP which is only servicing a non-critical function can jeopardize the security of our systems and data. Then I would have expected cyber security referred to in the enumeration of domains of which risks are analysed, through due diligence.

**Rule 33 -**Should we consider it is covered under the "operational risks" term in paragraph 32? But, in that case, why to specifically refer to information security when considering a CSP servicing a critical or important function. This looks confusing.

Furthermore, in this section, it is again not referred to Data Protection. Should we understand it is covered by Information Security ?

Finally, we understand that, while it is possible to know if the same CSP is used by different business units within the firm, it is not clear how the firm can know the concentration within the sector as, to obtain that information, it might require the input from external firms. We would like to have clarification to this point.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Agree

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

Agree

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

Yes we agree, however, **rule 46** is not clear. Maybe it should be re-phrased to make it more concrete.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

**We do not agree**

**Rule 48 -** This rule looks too restrictive. We should be able to exercise our access and audit rights, whatever the criticality of the function supported by the CSP. From a practical point of view, it is not manageable to arrange our contractual audit clause, depending whether the outsourcing is related to a critical or important function or not.

**Rule 51 -** We wonder how to deal with those CSPs that do not accept the expansion of the scope or to perform on-site audits. CSPs like Microsoft do not accept these contractual clauses. We would like to have a clarification on how to deal with this type of suppliers.

**Rule 51 d) & e) -** This is not workable. We are (and will never be) in position to assess qualifications, expertise or performance of an external auditor/certifier and/or its output. Certaily not, if this auditor/certifier only occasionally works with the Bank. As regards auditors, they can be appointed by the Bank. Then the qualifications assessment is logically part of the procurement process. But certifiers are mostly chosen by the CSP itself, even before they contract with the Bank. Then such assessment of the expertise of the cerifying entity is not feasible.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

We agree

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

We are not agree:

**Rule 57 -** We consider "in a timely manner" too broad and open to interpretation. It could mean from every time there is a new outsourcing to a period the firm consider adequate (e.g. once a year).

**Rule 58** - Again (see comment about rule 29 above), it should probably be useful to also monitor from where data can be accessed.

<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>

**NA,** This is for the competent authorities

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

**NA,** This is for the competent authorities

<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>

Comment: One-off: the effort would probably be in the inventory of the cloud computing solutions used at the Bank and their mapping with critical and important functions. The question remains, from a security point of view, whether the proportionality rule should only refer to the criticality / importance of the function served.

In the run: most of the requirements are of common sense and we already comply with them.

<ESMA\_QUESTION\_COGL\_12>