|  |
| --- |
| 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 | McAfee |
| Activity | Non-financial counterparty |
| Are you representing an association? |  |
| Country/Region | International |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

In the definitions on page 13, the definition for cloud computing includes “software and applications” (SaaS). However, many of the regulations appear to only consider infrastructure and platform (IaaS and PaaS) as a service and ignore software as a service.

However, major dangers are contained within outsourcing to SaaS cloud computing, especially around information security as the capabilities within SaaS services can include sharing and collaboration outside regulated organisations.

In many cases we observe that cloud services are construed as a replacement for a bank’s data center’s, which is an over-simplification. In addition, there is an absence of guidelines setting our user and access control.

Our responses and recommendations contained in our response aim to ensure that SaaS is included as part of the guideline, and that the principle of a shared responsibility model between banks and their could service providers (CSPs) is the basis of any guidance.

<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>

Paragraph 28 add

‘The register should include all cloud arrangements, including those that are created by individual departments and individual employees.’

Paragraph 29add to (g)

‘And dispute resolution mechanism and any statute of limitations.’

Para graph 29 add to (o)

‘Security functions provided by the CSP, such as encryption strength at rest, encryption strength in transit, most recent penetration testing date, application security vulnerability protection, CVE vulnerabilities.’

Paragraph 29add to (p)

‘Data retention policy upon account termination’.

Paragraph 29 add to (q)

‘Authentication capabilities. Anonymous use, support for multi-factor authentication, integration with enterprise identity and federation methodologies supported’.

Paragraph 29 add to (r)

‘Support for logging of admin, user and data activity’

Explanation

The additions to paragraph 28 are to address instances in which companies can be at risk from an individual group or employee outsourcing that is not centralised and controlled. So called “shadow IT” can include software engineers starting their own IaaS efforts or LOB or individuals using commercial SaaS services without realising the dangers of unfettered access, sharing and collaboration. Shadow IT usage can have major security risks for banking organisations.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

We would recommend that the management of these registers is also in compliance with existing sectorial or horizontal legal requirements. CSPs and banking face different requirements under national and/ or EU legislation (i.e. data breach notification under GDPR, incident reporting obligation under the NIS Directive, and PSD2 requirements).

<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>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Regarding paragraph 41 (j), CSPs should not be obligated to submit confidential internal audit reports to a client, the industry standard security reports should suffice.

In paragraph 41 (n), contractual arrangements may, in some cases, not permit customers to audit the premises of the CSP. In general, customers should also rely on the results of independent third-party audits and regular compliance questionnaires provided by the customer to the CSP (see also our remarks on Q7 on audit rights).

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

Paragraph 43 add

‘(i) A firm should evaluate all of the cloud functionality and ensure implementation of strong information security functions to minimise possible data loss. Companies should implement data loss prevention (DLP) measures such as user access, device control, user identification, user logging, user behaviour anomaly detection, user controls for internal and external data sharing via cloud, all cloud functions, cloud to cloud traffic capabilities, data minimisation, user privilege controls, audit of cloud configurations and cloud configuration drift over time.’

Explanation:

While cloud service providers are responsible for security OF the cloud, it is the enterprises who are responsible for data IN the cloud. The regulated organisations need to understand and take responsibility for data transferred TO clouds, when data is INSIDE clouds, being transferred BETWEEN clouds and when downloaded FROM cloud computing to either their own employees or third-party collaborators.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

We recognize and support that financial firms would need to have more extensive audit rights., however we do not agree that a financial firm should have unlimited access/ audit rights.

In addition, at paragraph 56 we would recommend adding

‘Sub-outsourcing is in effect if a cloud service provider (CSP) uses the hosting services of another CSP. For example; if a SaaS provider hosts their service on AWS, that should be made clear to the customer organisation and any material change (such as moving from AWS to Azure) must be communicated to the customer.’

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_12>