|  |
| --- |
| 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 | TAS Group. |
| Activity | Other Financial service providers |
| Are you representing an association? |[ ]
| Country/Region | Europe |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

This document is TAS Group’s response to ESMA’s request for comments on the “Consultation Paper on Draft Guidelines on Outsourcing to Cloud Service Providers”.

TAS Group is a Fintech Provider specialized in software solutions for e-money, payments and financial markets, listed on the Milan Stock Market since May 2000 and leader in Italy in card management systems, access to payment networks and treasury liquidity management.

TAS Group is the commercial name that identifies the group of companies constituted by TAS S.p.A. - controlled by OWL S.p.A. - and by its subsidiaries Global Payments S.p.A., MANTICA ITALIA Srl and TAS International SA. The latter in turn controls the companies TAS France SASU, TAS Iberia S.L.U., TAS Germany GmbH, Infraxis AG, TAS Eastern Europe d.o.o, TASamericas Ltda and TAS USA Inc.

TAS Group serves the most important commercial and central banks in Italy and Europe, the major financial services centres and some of the main global broker dealers present in the Fortune Global 500 ranking.

Operating through its subsidiaries, TAS Group proposes itself as a first level partner also on the international market.

<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>

A firm should have a fully comprehensive view of its cloud outsourcing strategy. In support of such strategy the firm should have clearly defined its approach concerning which functions may be outsourced, regardless of any of these being considered critical or important, how such functions impact the firm’s business, its legal aspects and also its reputation.

The firm should

* define a process concerning such topics, have it approved by its management and strictly follow it; the process should be based on internal policies, procedures, checklists;
* assign the relevant responsibilities to its personnel, who in turn should acknowledge that the process has been understood and will follow it;
* maintain clear evidence of abiding to the process.

In support of a risk-based approach, the firm should choose the CSP (Cloud Service Provider) after having defined and listed the functions they intend outsourcing and which legal, financial and reputational impacts these functions may require.

Upon such a list investigate as to which CSPs are available in the market and for each of these gain a clear view of their services, any relevant legal requirements, how such services match the firm’s needs and also the complexities involved in understanding how the services are delivered by the CSP, when compared to the firm’s needs and compared to the case where the firm would carry out the services internally.

The choice of the specific CSP and the relevant contractual characteristics are also fundamental when carrying out a due diligence concerning a CSP.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

The firm should have an asset listing of all of its scopes and functions, regardless of whether the function is outsourced by a CSP, or if it is delivered internally by the firm. The listing should provide evidence defining whether the function is critical or non-critical, if it is internal, and as such to be considered as a cost for the firm’s business, or if it is for an external customer providing revenues.

The asset listing should be maintained updated so that it may be of prompt reference in case of need, implying that the firm should appoint this responsibility to a staff member.

Each item in the asset list should be described as thoroughly as possible, so as to avoid missing out in some of its details.

The firm should define and approve a process to be followed concerning cloud outsourcing based on internal policies, procedures, checklists clearly describing the process flow and assigning responsibilities to its personnel.

<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>

Before the firm decides to enter into a cloud service provisioning agreement, a list of business requirements should be carried out, listing which functions are included in its business and out of these, which are internal / external, which are critical to its business from different point of views, such as but not limited to operational risks, reputation, legal aspects and conflicts of interests.

A pre-outsourcing analysis should be carried out at regular intervals, not only when evaluating a CSP and whenever the firm deems necessary such as in cases of specific events requiring the cloud outsourcing of the functions to be reviewed over again.

Such analysis, should detail what the market has to offer as far as cloud service provisioning is concerned, so that the firm may gain as much as possible insight and a clear view regarding the decision to outsource some of its functions.

To achieve the above, the firm should define a list of requirements and list the functions that may be outsourced to the cloud. Such list should be used to evaluate CSPs, their relevant services, how these are delivered, how easy or complex such services are when compared to how the firm would operationally carry out the same services internally by themselves, the CSP’s geographical position, any political restrictions which may apply, as well as any reputational impacts that may arise from outsourcing the service to a CSP and the contractual / legal requirements that may be applicable to the outsourced function.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

The firm should pay particular attention when considering the contractual aspects with the CSP. The agreement should clearly outline details of the firm and the CSP and the firm should also seek to gain evidence concerning:

* the CSP’s service providers, without limiting this investigation to the firm’s services being delivered, but aiming to gain as much insight as possible on the CSP,
* if sub-outsourcers are involved and to which extent,
* whether the CSP, or any sub-outsourcer and / or any CSP’s service provider will have access to the firm’s data and for what reason, so as to comply with the data privacy regulation requirements.

All of the above should be clearly specified by the firm in its internal policies, procedures and checklists.

Once knowledge on the above is clear, the firm should move forward considering other aspects of the contract, such as details concerning:

* how the CSP guarantees its business continuity,
* details of a disaster recovery site and when the site is used,
* which SLA’s are foreseen,
* the risk management approach adopted by the CSP.

The firm should also not underestimate the fact that the bigger the CSP, the lower the margins will be when requesting adjustments or variations to the contractual requirements.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

Information security is important, even more when a CSP is involved in the information process flow and its management.

The firm should define its information security approach by means of internal policies, procedures and any relevant supporting document. The definition and maintenance of such document kit should:

* be assigned to a senior member of the staff, who in turn may rely on a team knowledgeable on information security topics,
* be reviewed and disseminated within the firm at regular intervals, or when deemed necessary, such as in cases of significant changes within the information security scope,
* be made available for any references to its personnel, who in turn acknowledge to have understood and duly abide to its contents.

In case of a function being outsourced to a CSP, the information security document kit should also include topics, such as:

* a due diligence on the CSP, aiming to gain knowledge on the CSP’s information security approach,
* any geographical, legal, political and reputational aspects concerning the CSP, which may impact the firm’s information security requirements,
* the need for information security requirements to be included in the contractual agreement between the firm and the CSP.

In case any of the above topics are not supplied by the CSP, the firm’s risk management team should be involved.

Once the firm has obtained enough data on both its internal information security requirements and the chosen CSP’s, these should be reported in the written agreement, so that responsibilities should be clear to both parties and the relevant monitoring tasks to protect the services sensitive data may be set forth on a regular basis.

The firm should allocate knowledgeable personnel to cover all its internal information security scopes and tasks and at the same time, allocate knowledgeable personnel to ensure the established information security requirements between the firm and the CSP for the specific outsourced function are maintained.

Topics such as:

- infrastructure hardening, ranging from Hardware to application Software, including operating systems and middleware should be guaranteed within all of the firm’s scope, regardless of a function being delivered internally by the firm or externally by a CSP;

- multi-factor authentication criteria should be applied to any access being requested to the firm’s infrastructure, independent of whether the function is being delivered internally by the firm or by a CSP;

- data protection by means of encryption should be applied on all network links, regardless of whether these are internal or external to the firm, and when data is at rest either in a Data Base Management System (DBMS) or in any other type of repository, including backups;

- encryption keys used to protect data, should be managed by means of HSMs (Hardware Security Modules) and under dual control and split knowledge criteria; encryption keys should be:

- generated using accepted strong cryptographic processes,

- distributed to the minimum number of actors / parties as possible and according to a predefined secure process,

- stored securely, either in a SCD (Secure Cryptographic Devic) or encrypted under relevant key encryption keys,

- rotated once the cryptoperiod has been reached or the specified amount of cypher-text has been produced,

- replaced in case of evidence that the key has been weakened;

furthermore the firm should have a process in place to prevent unauthorised substitution of data encryption keys; the firm should specify all of the above in its internal policies and procedures, allocating relevant roles and responsibilities to knowledgeable personnel and ensuring that the proper requirements have been specified in the written agreement, in case the CSP is involved in any encryption keys management tasks or operations; as HSM devices could be provided by the CSP, the firm should pay attention to the make and model of the HSMs and verify whether these suit the firm’s needs and also verify if the devices compliance characteristics, including remaining support periods before the end of life milestone of the device, are adequate to the firm’s needs;

- the firm should strive to ensure that:

- the Software used in its scopes follows a Secure Software Development Life Cycle (SSDLC),

- the SSDLC, regardless of whether applicable to internal personnel or to a Third Party includes Secure Coding features such as training and static and dynamic code reviewing,

- all steps in the SSDLC are traced and all documental evidences are maintained;

- Service level agreements are adequately based on the outsourced function requirements; SLA’s should be monitored by the firm’s personnel and include business continuityfeatures,applicable in case of any need, such as natural disasters or any other type of error that may incur in the CSP’s service delivery;

- geographic location of the CSP should be taken into consideration as per the firm’s risk management approach;

- the CSP’s service delivery should be constantly monitored by the firm, so as to ensure the firm’s compliance towards any competent authority and any applicable international security standard; the firm should strive to gain as much possible evidence regarding the services being delivered by the CSP, so to be able to provide the necessary documental evidences to competent authorities, or any governing body responsible for any applicable security standards.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

The firm should evaluate the impacts that an exit strategy may have on the functions that they are planning to outsource and consider the relevant risks and business impacts involved.

Exit strategies should be included in the CSP’s due diligence process and also be included in the written agreement between the firm and the CSP. The written agreement should clearly state that in such an event, the CSP, and if applicable its service providers or its sub-outsourcers, will efficiently cooperate in the transition plan, securely delete all relevant data from its infrastructure and provide adequate documental evidence of this being done.

As exit strategies may have an important impact on the firm’s business, the firm should have policies, procedures, checklists and other supporting documents specifically defined on such topic. Such documents should also include the justification for an exit strategy, defining a list of possible events that may trigger the evaluation concerning the change of the current CSP.

The firm should ensure that in case they decide to discontinue the agreement with the CSP, the impacts on the service should be as minimal as possible, aiming at best to have none.

Exit strategies risks should be overseen at regular intervals, as well as identifying any alternative or supporting tasks to be adopted in case of a change in the CSP, all with the aim of defining and testing a transition plan.

Policies and procedures on exit strategies should be reviewed and tested at regular intervals, to ensure that data confidentiality, integrity and availability will be maintained at all times.

The firm should allocate resources to define and maintain exit strategies documents and to disseminate the contents at regular intervals to the team allocated to such event.

The exit strategy team should receive reports from the firm’s service monitoring team on how the service is being delivered by the CSP. The exit strategy team should promptly analyse the reports seeking information leading to an exit strategy event.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

During the firm’s due diligence process on the potential CSP’s, the firm should gain knowledge concerning any access and audit rights restrictions from each CSP.

The firm should have policies and procedures defined concerning access and audit requirements and the firm’s due diligence process on the CSP should verify whether the CSP’s access and audit rights are compatible with the firm’s requirements. In case of compatibility then the firm and the CSP may move forward with the written agreement, in which at least the following should be stated:

* no limitations have been found concerning access and audit rights by the firm on the CSP’s premises,
* the events upon which the firm may request an on-site visit,
* the shortest period of time between a request and the on-site visit,
* who on behalf of the firm may request the on-site visit,
* who on behalf of the firm will gain access to the CSP’s premises and for what reason,
* list any certification that the CSP may have, which would suffice the firm’s requirements, requesting the CSP to maintain it in the future, or duly inform the firm otherwise.

The firm’s policies and procedures concerning such topic should outline that such exercise on behalf of the firm shall be carried out under timelines and modes agreed with the CSP and that any techniques used during the audit should not impact the CSP’s SLA’s or data confidentiality, integrity and availability pertaining to the firm’s functions or to any other CSP’s customer.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

In case sub-outsourcers are involved in the delivery of the firm’s functions by the CSP, the sub-outsourcer’s behaviour, as far as security, data confidentiality, integrity and availability is up to the CSP.

The firm should define in its policies whether:

* sub-outsourcers may be permitted in the delivery of the firm’s functions by the CSP
* to which extent, sub-outsourcers may be involved during the due diligence process on the CSP.

Regardless of whether sub-outsourcers are present when the due diligence process is carried out, the written agreement between the firm and the CSP should include responsibility clauses concerning sub-outsourcers involved in the delivery of the firm’s functions, specifying that sub-outsourcers behaviour is responsibility of the CSP, or if applicable, that no sub-outsourcer be involved in the delivery of their services by the CSP.

The firm should verify the above at regular intervals ensuring that the CSP adequately oversees their sub-outsourcers

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

Competent authorities need to have a comprehensive view of the firms’ critical or important functions that are being, or will be, outsourced, so that they may carry out an effective monitoring on the overall cloud outsourcing in the EU.

Each firm aiming to make use of CSP services, should provide competent authorities sufficient and up to date information regarding their critical or important functions which they intend outsourcing to CSPs.

<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>

Competent authorities need to have a comprehensive view of the firms’ critical or important functions in order to gain an effective and comprehensive view on the overall cloud outsourcing in the EU.

Competent authorities should use the information received by the firms, to assess the CSPs’ offerings in the EU, in terms of risk, fiscal aspects, compliance and security towards applicable international standards as well as the data privacy regulation.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

Overall a firm should strive to have a clear view on its internal processes. Such processes should be defined by means of policies, procedures and supporting documents, which should be:

* clear and easy to understand;
* defined by knowledgeable staff;
* reviewed at regular intervals or upon specific events.

The firm should allocate resources to assess compliance at regular intervals on the services being delivered, both internally and by CSPs’.

The firm should note that the bigger the CSP, the more difficult it will be to review contractual agreements in favour of the firm.

<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>

In the context of ESMA guide lines, TAS Group plays the role of the CSP and as such any information concerning costs is out of scope.

<ESMA\_QUESTION\_COGL\_12>