BSA Response to ESMA's Consultation on Draft Guidelines on Outsourcing to Cloud Service Providers

Brussels, 01 September 2020

Introductory comments
Question: Please make your introductory comments below, if any.
Answer: ***As a general remark, we would welcome any clarification on how do the current draft ESMA guidelines interplay with the existing EBA guidelines. As specific EU supervisory authority guidelines are already in place, would it be more efficient and easier to transact for the both Financial Services and the Cloud industry to follow one consistent set of guidelines, which already exists under the EBA guidelines?***

Guideline 1. Governance, oversight and documentation
Question 1: Do you agree with the suggested approach regarding a firm's governance and oversight in relation to its cloud outsourcing arrangements? Please explain. (see Annex starting as of page 5)
Answer: ***We generally agree with the suggested approach regarding the governance and oversight guidelines for financial services' organizations, i.e. on the assignment of responsibilities, the allocation of sufficient resources, the accountability of management, the introduction of a risk-based approach and the maintenance of an updated register of the Cloud outsourcing arrangements.***

Guideline 1. Governance, oversight and documentation
Question 2: Do you agree with the suggested documentation requirements? Please explain. (see Annex starting as of page 5)
Answer: ***Regarding the criteria for the management of the critical CSPs register, we would recommend clarifying that the organizations ensure that the management of these registers is also in compliance with existing sectorial or horizontal legal requirements. Often organizations – CSPs and customers alike – may have to face different requirements under national and/ or EU legislation (i.e. data breach***

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

notification under GDPR, incident reporting obligation under the NIS Directive, and PSD2 requirements).

Guideline 3. Contractual requirements
Question 4: Do you agree with the suggested contractual requirements? Please explain. (see Annex starting as of page 5)
Answer: ***Regarding the requirements laid down in paragraph 41, it is necessary to ensure that all they are all compliant with existing EU acquis (or their national transposition in the selected jurisdiction, thereof). For instance point (k) mentions "the obligation for the CSP to report incidents", however the existing requirements under Article 14 of the NIS Directive would require of the data controller (the customer) to report severe incidents to the competent authority. Against this background, contractual obligations between technology providers and their regulated customers often forbid the former to report incidents on behalf of the latter, and instead focus on clarifying the supporting activities of the CSP in assisting its customer in the incident management and reporting. We would recommend an amendment of this subsection in the following general spirit:*** "k) provisions regarding the management of incidents by the CSP, including the obligation ***under appropriate circumstances*** for the CSP to report significant incidents ***to the firm***" ***Regarding paragraph 41 (j), we believe that CSPs should not be obligated to submit confidential internal audit reports to a client, the industry standard security reports should suffice.*** ***Paragraph 41 (f) is potentially problematic because it essentially introduces a notice and consent regime for the addition of any new data centers. It also would allow for each customer to set up unique conditions that must be met before data centers could be added rather than having a single standard. Also, a mechanism for notifying customers of new data centres that come online prior to these being activated, is potentially difficult to implement.*** ***On 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).***

Guideline 4. Information security
Question 5: Do you agree with the suggested approach regarding information security? Please explain. (see Annex starting as of page 5)
Answer: ***Paragraph 43 (c) suggests that firms consider "appropriate key management solutions to limit the risk of non-authorised access to the encryption keys (for example by preventing the CSP from storing and managing encryption keys or requiring separation of duties between key management and operations)." For technical reasons, CSPs may***

be unable to relinquish access to encryption keys, therefore such requirements should remain in their current, non-prescriptive form.

Except for the above point, we would generally agree with these requirements. Financial services' entities are undergoing digital transformation to improve and increase efficiency of their data processing, data storage and infrastructure management, including through the uptake of cloud services. They should take all appropriate measures related to risk mitigation and management to increase their operational resilience through a principle-based, outcome-oriented and technology neutral risk management approach. In addition to the suggested measures, such could non-exhaustively include: a security risk management framework; a contingency plan; reporting and / or incident response protocols; the deployment of threat detection and mitigation tools.

Guideline 6. Access and audit rights
Question 7: Do you agree with the suggested approach regarding access and audit rights? Please explain. (see Annex starting as of page 5)
Answer: ***We recognize that financial firms would need to have more extensive audit rights. However, we need to keep in mind the amount of disruption audits could cause for CSPs and that there should be some say for CSPs in how they are conducted. A financial firm shouldn't have unlimited access/ audit rights downstream, and point 49 seems to provide a helpful clarification in that regard. In addition, CSPs should not be prohibited from charging the audit costs to their customers, given the high fees and disruptive potential some audits bring.*** ***The inclusion of a contractual right to request expansion of audit scope as suggested by point 51 (f)) seems quite constraining. If such a right were granted to firms, the CSP should have the right to decline such expansion and terminate the agreement. If expansion would be requested, firms should also have to incur the cost of any additional audits/ certifications (including the hiring of any additional personnel required to maintain such compliance). Financial firms should also have discretion over the fact that they should or should not rely on certifications and audit reports over time (point 52), or at least should be able to address it with the CSP.***

Guideline 7. Sub-outsourcing
Question 8: Do you agree with the suggested approach regarding sub-outsourcing? Please explain. (see Annex starting as of page 5)
Answer: ***In paragraph 55 points (d), (e) and (f), the whole term/ concept of sub-outsourcer is not clear enough. Regarding paragraph 55 (e), it is important to keep the optionality ("or that explicit approval is required…") so that Cloud providers do not have to rely exclusively on explicit approval. For example, CSP customers should not have the***

right to object or approve a CSP's use of sub-outsourcers or sub-contractors. As long as the CSP is compliant with the agreement terms then the CSP can determine which sub-outsourcers or sub-contractors it wants to use.

Guideline 9. Supervision of cloud outsourcing arrangements
Question 10: Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain. (see Annex starting as of page 5)
Answer: ***Paragraph 59's reference to risk assessment by competent authorities is quite broad and could potentially cover a wide range of different actions by different supervisors. It would be helpful to have some more delineation of what this assessment could/ should contain.***

Guideline 9. Supervision of cloud outsourcing arrangements
Question 12: 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 organisation, where relevant. (see Annex starting as of page 5)
Answer: ***While this question seems very much aimed at financial firms only, we would like to highlight that there are financial and operational benefits and efficiencies of moving to cloud, therefore cloud outsourcing should not be overlooked.***

ANNEX: Draft ESMA Guidelines on outsourcing to cloud services providers

(full document available here)

Guideline 1. Governance, oversight and documentation

25. A firm should have a defined and up to date cloud outsourcing strategy that is consistent with the firm's relevant strategies, such as information and communication technology strategy, information security strategy, operational risk management strategy, and internal policies and processes.

26. A firm should:
    a) clearly assign the responsibilities for the documentation, management and control of cloud outsourcing arrangements within its organisation;
    b) allocate sufficient resources to ensure compliance with these guidelines and all of the legal requirements applicable to its cloud outsourcing arrangements;
    c) establish an outsourcing oversight function or designate a senior staff member who is directly accountable to the management body and responsible for managing and overseeing the risks of cloud outsourcing arrangements. When complying with this guideline, firms should take into account the nature, scale and complexity of their business and the risks inherent to the outsourced functions and make sure that their management body has the relevant technical skills[1]. Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and control of cloud outsourcing arrangements.

27. On a risk-based approach, a firm should monitor on an ongoing basis the performance of activities, the security measures and the adherence to agreed service levels by its CSPs. The primary focus should be on the outsourcing of critical or important functions.

28. A firm should maintain an updated register of information on all its cloud outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. When distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements, it should provide a brief summary of the reasons why the outsourced function is or is not considered critical or important. Taking into account national law, a firm should also maintain a record of terminated cloud outsourcing arrangements for an appropriate time period.

[1] For investment firms and credit institutions, see the 'Joint ESMA and EBA guidelines on the assessment of suitability of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU' (EBA/GL/2017/12).

29. For the cloud outsourcing arrangements concerning critical or important functions, the register should include at least the following information for each cloud outsourcing arrangement:
    a) a reference number;
    b) the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the CSP and for the firm;
    c) a brief description of the outsourced function, including the data that is outsourced and whether this data includes personal data (for example by providing a yes or no in a separate data field);
    d) a category assigned by the firm that reflects the nature of the function referred to under point (c) (for example information technology, control function), which should facilitate the identification of the different types of cloud outsourcing arrangements; e) whether the outsourced critical or important function supports business operations that are time-critical;
    f) the name and the brand name (if any) of the CSP, the country of registration, the corporate registration number, the legal entity identifier (where available), the registered address, the relevant contact details and the name of the parent company (if any);
    g) the governing law of the cloud outsourcing arrangement and, if any, the choice of jurisdiction;
    h) the cloud deployment models and the specific nature of the data to be held and the locations (namely countries) where such data may be stored and processed;
    i) the date of the most recent assessment of the criticality or importance of the outsourced function and the date of the next planned assessment;
    j) the date of the most recent risk assessment/audit together with a brief summary of the main results, and the date of the next planned risk assessment/audit;
    k) the individual or decision-making body in the firm that approved the cloud outsourcing arrangement;

    l) where applicable, the names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the countries where the sub-outsourcers are registered, where the sub-outsourced service will be performed, where the data will be stored and where the data may be processed;
    m) the estimated annual budget cost, excluding VAT, of the cloud outsourcing arrangement.

30. For the cloud outsourcing arrangements concerning non-critical or non-important functions, a firm should define the information to be included in the register on the basis of the nature, scale and complexity of the risks inherent to the outsourced function.

Q1: Do you agree with the suggested approach regarding a firm's governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

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

Guideline 2. Pre-outsourcing analysis and due diligence

31. Before entering into any cloud outsourcing arrangement, a firm should:

a) assess if the cloud outsourcing arrangement concerns a critical or important function;

b) identify and assess all relevant risks of the cloud outsourcing arrangement;

c) undertake appropriate due diligence on the prospective CSP;

d) identify and assess any conflict of interest that the outsourcing may cause.

32. In general, the pre-outsourcing analysis and due diligence should be proportionate to the nature, scale and complexity of the function that the firm intends to outsource and the risks inherent to this function. It should include at least an assessment of the potential impact of the cloud outsourcing arrangement on the firm's operational, legal, compliance, and reputational risks.

33. In case the cloud outsourcing arrangement concerns critical or important functions, a firm should also:

a) assess all relevant risks that may arise as a result of the cloud outsourcing arrangement, including risks in relation to information and communication technology, information security, business continuity, legal and compliance, reputational risks, operational risks, and possible oversight limitations for the firm, arising from:

i. the selected cloud service and the proposed deployment models;

ii. the migration and/or the implementation processes;

iii. the sensitivity of the function and the related data which are under consideration to be outsourced (or have been outsourced) and the security measures which would need to be taken;

iv. the interoperability of the systems and applications of the firm and the CSP, namely their capacity to exchange information and mutually use the information that has been exchanged;

v. the portability of the data of the firm, namely the capacity to easily transfer the firm's data from one CSP to another;

vi. the political stability, the security situation and the legal system (in particular the law, including insolvency law and enforcement as well as the requirements concerning the confidentiality of the firm's business related and/or personal data) of the countries (within or outside the EU) where the outsourced functions would be provided and where the outsourced data would be stored; in case of sub-outsourcing, the additional risks that may arise if the sub-

outsourcer is located in a third country or a different country from the CSP and, in case of a sub-outsourcing chain, any additional risk which may arise, including in relation to the absence of a direct contact between the firm and the sub-outsourcer performing the outsourced function;

vii. possible concentration within the firm (including, where applicable, at the level of its group,) caused by multiple cloud outsourcing arrangements with the same CSP as well as possible concentration within the sector, caused by multiple firms making use of the same CSP or a small group of CSPs. When assessing the concentration risk, the firm should take into account all its cloud outsourcing arrangements (and, where applicable, the cloud outsourcing arrangements at the level of its group) with that CSP;

b) take into account the expected benefits and costs of the cloud outsourcing arrangement, including weighing any significant risks which may be reduced or better managed through the outsourcing against any significant risks which may arise as a result of the proposed cloud outsourcing arrangement.

34. In case of outsourcing of critical or important functions, the due diligence should include an evaluation of the suitability of the CSP. When assessing the suitability of the CSP, a firm should ensure that the CSP has the business reputation, the skills, the resources (for example human, IT and financial), the organisational structure and, if applicable, the regulatory authorisation(s) or registration(s) to perform the critical or important function in a reliable and professional manner and to meet its obligations over the duration of the cloud outsourcing arrangement. Additional factors to be considered in the due diligence on the CSP include, but are not limited to:

a) the management of information security and the protection of personal data;

b) the service support, including support plans and contacts, and incident management processes;

c) the business continuity and disaster recovery plans;

35. Where appropriate and in order to support the due diligence performed, a firm may also use certifications based on international standards and external or internal audit reports.

36. A firm should reassess the criticality or importance of a function previously outsourced to a CSP periodically and every time there is a material change in relation to the nature, scale or complexity of the risks inherent to the cloud outsourcing arrangement.

37. If the firm becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the CSP, the pre-

outsourcing analysis and due diligence on the CSP should be promptly reviewed or re-performed.

38. The due diligence on the CSP should be performed prior to outsourcing any function thereto. In case the firm enters into an additional arrangement with a CSP that has already been assessed, the firm should determine, on a risk-based approach, whether a new due diligence is needed.

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.

Guideline 3. Contractual requirements

39. The respective rights and obligations of a firm and of its CSP should be clearly allocated and set out in a written agreement.

40. The written agreement should expressly allow the possibility for the firm to terminate it, where necessary.

41. In case of outsourcing of critical or important functions, the written agreement should set out at least:

a) a clear description of the outsourced function;

b) the start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the firm;

c) the governing law of the agreement and, if any, the choice of jurisdiction;

d) the parties' financial obligations;

e) whether the sub-outsourcing of critical or important functions (or material parts thereof) is permitted, and, if so, the conditions to which the sub-outsourcing is subject, having regard to Guideline 7;

f) the location(s) (namely countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s);

g) provisions regarding information security and personal data protection, having regard to Guideline 4;

h) the right for the firm to monitor the CSP's performance on a regular basis;

i) the agreed service levels, which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

j) the reporting obligations of the CSP to the firm and, as appropriate, the obligations to submit reports relevant for the firm's security function and key

functions, such as reports prepared by the internal audit function of the CSP;

k) provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report incidents;

l) whether the CSP should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

m) the requirements for the CSP to implement and test business continuity and disaster recovery plans;

n) the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access ('access rights') and to inspect ('audit rights') the books, premises, relevant systems and devices of the CSP to the extent necessary to monitor the CSP's performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6;

o) provisions to ensure that the data owned by the firm can be recovered by the firm as needed, having regard to Guideline 5.

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

Guideline 4. Information security

42. A firm should set information security requirements in its internal policies and procedures and within the cloud outsourcing written agreement and monitor compliance with these requirements on an ongoing basis, including to protect confidential, personal or otherwise sensitive data.

43. For that purpose, in case of outsourcing of critical or important functions, a firm, applying a risk-based approach, should at least:

a) *information security organisation:* ensure that there is a clear allocation of information security roles and responsibilities between the firm and the CSP, including in relation to threat detection, incident management and patch management, and ensure that the CSP is effectively able to fulfil its roles and responsibilities;

b) *access management*: ensure that strong authentication mechanisms (for example two factor authentication) are implemented and that access controls appropriately prevent unauthorised access to the firm's data and back-end cloud resources;

c) *encryption and key management:* consider the use of encryption technologies, where necessary, for data in transit, data in memory, data at rest and data backups, in combination with appropriate key management solutions to limit the risk of non-authorised access to the encryption keys (for example by preventing the CSP from storing and managing encryption keys or requiring separation of duties between key management and operations);

d) *operations and network security:* consider appropriate levels of segregating networks (for example tenant isolation in the shared environment of the cloud, operational separation as regards the web, application logic, operating system, network, Data Base Management System (DBMS) and storage layers) and processing environments (for example test, User Acceptance Testing, development, production)

e) *application programming interfaces (API):* consider mechanisms for the integration of the cloud services with the systems of the firm to ensure security of APIs (for example establishing and maintaining information security policies and procedures for APIs across multiple system interfaces, jurisdictions, and business functions to prevent unauthorised disclosure, modification or destruction of data);

f) *business continuity and disaster recovery*: ensure that effective business continuity and disaster recovery controls are in place (for example by setting minimum capacity requirements, selecting hosting options that are geographically spread or requesting and reviewing documentation showing the transport route of the firm's data between the CSP's systems, as well as considering the possibility to replicate machine images to an independent storage location);

g) *data location*: adopt a risk-based approach to data storage and data processing location(s) (namely country or region);

h) *compliance & monitoring*: ensure that the CSP complies with internationally recognised information security standards and has implemented appropriate information security controls (for example by requesting the CSP to provide evidence that it conducts relevant information security reviews and by performing regular assessments and tests on the CSP's information security arrangements).

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

Guideline 5. Exit strategies

44. In case of outsourcing of critical or important functions, a firm should ensure that it is able to exit cloud outsourcing arrangements without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with the applicable legal requirements, as well as the confidentiality, integrity and availability of its data. To achieve this, a firm should:

a) develop and implement exit plans that are comprehensive, documented and sufficiently tested. These plans should be updated as needed, including in case of changes in the outsourced function;

b) identify alternative solutions and develop transition plans to remove the outsourced function and data from the CSP and, where applicable, any sub-outsourcer, and transfer them to the alternative CSP indicated by the firm or directly back to the firm. These solutions should be defined with regard

to the challenges that may arise from the location of the data, taking the necessary measures to ensure business continuity during the migration phase;

c) ensure that the cloud outsourcing written agreement includes an obligation for the CSP to orderly transfer the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy;

d) ensure that any data removed or transferred is securely deleted from the systems of the CSP and, where applicable, of any sub-outsourcer (for example, by requesting a written confirmation by the CSP).

45. When developing the exit plans and solutions referred to in points (a) and (b) above ('exit strategy'), the firm should consider the following: a) define the objectives of the exit strategy;

b) define the trigger events that could activate the exit strategy. These should include at least the termination of the cloud outsourcing arrangement at the initiative of the firm or the CSP and the failure or other serious discontinuation of the business activity of the CSP;

c) perform a business impact analysis that is commensurate to the function outsourced to identify what human and other resources would be required to implement the exit strategy;

d) assign roles and responsibilities to manage the exit strategy;

e) test the exit strategy, using a risk-based approach;

f) define success criteria of the transition.

46. The firm should include indicators of the trigger events of the exit strategy in its ongoing monitoring and oversight of the services provided by the CSP.

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

Guideline 6. Access and audit rights

47. A firm should ensure that the cloud outsourcing written agreement does not limit the firm's effective exercise of the access and audit rights as well as its oversight options on the CSP.

48. A firm should ensure that the exercise of the access and audit rights (for example, the audit frequency and the areas and services to be audited) takes into consideration whether the outsourcing is related to a critical or important function, as well as the nature and extent of the risks and impact arising from the cloud outsourcing arrangement on the firm.

49. In case the exercise of the access or audit rights, or the use of certain audit techniques create a risk for the environment of the CSP and/or another CSP's client (for example by impacting service levels, confidentiality, integrity and availability of data), the firm and the CSP should agree on alternative ways to provide a similar result (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the CSP).

50. Without prejudice to their final responsibility regarding cloud outsourcing arrangements, in order to use audit resources more efficiently and decrease the organisational burden on the CSP and its clients, firms may use:

a) third-party certifications and external or internal audit reports made available by the
CSP;

b) pooled audits performed jointly with other clients of the same CSP or pooled audits performed by a third-party auditor appointed by multiple clients of the same CSP.

51. In case of outsourcing of critical or important functions, a firm should make use of the third-party certifications and external or internal audit reports referred to in paragraph 50(a) only if it:

a) ensures that the scope of the certifications or the audit reports covers the CSP's systems (for example processes, applications, infrastructure, data centres), the key controls identified by the firm and the compliance with the relevant legal requirements;

b) thoroughly assesses the content of the certifications or audit reports on a regular basis and verify that the certifications or reports are not obsolete;

c) ensures that the CSP's key systems and controls are covered in future versions of the certification or audit report;

d) is satisfied with the certifying or auditing party (for example with regard to its qualifications, expertise, re-performance/verification of the evidence in the underlying audit file as well as rotation of the certifying or auditing company);

e) is satisfied that the certifications are issued and that the audits are performed according to appropriate standards and include a test of the effectiveness of the key controls in place;

f) has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP;

g) retains the contractual right to perform individual on-site audits at its discretion with regard to the outsourced function.

52. In any case, the firm should assess whether the third-party certifications and external or internal audit reports are adequate and sufficient to comply with its regulatory obligations and, should not solely rely on these certification and reports over time.

53. A firm should ensure that, before a planned on-site visit, including by a third party appointed by the firm (for example an auditor), prior notice within a reasonable time period is provided to the CSP, unless an early prior notification is not possible due to an emergency or crisis situation. Such notice should include the location, purpose of the visit and the personnel that will participate to the visit.

54. Considering that cloud solutions present a high level of technical complexity and raise specific jurisdictional challenges, the staff performing the audit – being the internal auditors of the firm or a pool of auditors acting on its behalf – should have the right skills and knowledge to properly assess the relevant cloud solutions and perform effective and relevant audit. This should also apply to the firms' staff reviewing the certifications or audit reports provided by the CSP.

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

Guideline 7. Sub-outsourcing

55. If sub-outsourcing of critical or important functions (or a part thereof) is permitted, the cloud outsourcing written agreement between the firm and the CSP should:

a) specify any part or aspect of the outsourced function that are excluded from potential sub-outsourcing;

b) indicate the conditions to be complied with in case of sub-outsourcing;

c) specify that the CSP is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the CSP and the firm are continuously met;

d) include an obligation for the CSP to notify the firm of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm. The notification period to be set should allow the firm sufficient time to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them, as indicated in point (e) below;

e) ensure that the firm has the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect;

f) ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing, i.e. where the CSP proceeds with the sub-outsourcing without

notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement.

56. The firm should ensure that the CSP appropriately oversees the sub-outsourcer.

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

Guideline 8. Written notification to competent authorities

57. In case of planned outsourcing of critical or important functions, a firm should notify its competent authority in a timely manner.

58. The firm's written notification should include, taking into account the principle of proportionality, at least the following information: a) a description of the outsourced function;

b) the start date of the cloud outsourcing agreement and, as applicable, the next contract renewal date, the end date and/or notice periods for the CSP and for the firm;

c) the name and the brand name (if any) of the CSP, the country of registration, the corporate registration number, the legal entity identifier (where available), the registered address, the relevant contact details, and the name of the parent company (if any);

d) the governing law of the cloud outsourcing agreement and, if any, the choice of jurisdiction;

e) the cloud deployment models and the specific nature of the data to be held by the CSP and the locations (namely countries) where such data may be stored and processed;

f) where applicable, the names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the country or region where the sub-outsourcers are registered, where the sub-outsourced service will be performed, where the data will be stored and where the data may be processed;

g) a summary of the reasons why the outsourced function is considered critical or important;

h) the date of the most recent assessment of the criticality or importance of the outsourced function;

i) the date of the most recent risk assessment/audit together with a brief summary of the main results, and the date of the next planned risk assessment/audit;

j) the individual or decision-making body in the firm that approved the cloud outsourcing arrangement.

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

Guideline 9. Supervision of cloud outsourcing arrangements

59. Competent authorities should assess the risks arising from firms' cloud outsourcing arrangements as part of their supervisory process. In particular, this assessment should focus on the arrangements that relate to the outsourcing of critical or important functions.

60. Competent authorities should be satisfied that they are able to perform effective supervision, in particular when firms outsource critical or important functions that are performed outside the EU.

61. Competent authorities should assess on a risk-based approach whether firms:

a) have in place the relevant governance, resources and operational processes to appropriately and effectively enter into, implement, and oversee cloud outsourcing arrangements;

b) identify and manage all relevant risks related to cloud outsourcing.

62. Where concentration risks are identified, competent authorities should monitor the development of such risks and evaluate both their potential impact on other firms and the stability of the financial market.

Q10: Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

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

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 organisation, where relevant.

Appendix 1 - Summary of 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.

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

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.

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

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

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

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

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

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

Q10: Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

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

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 organisation, where relevant.