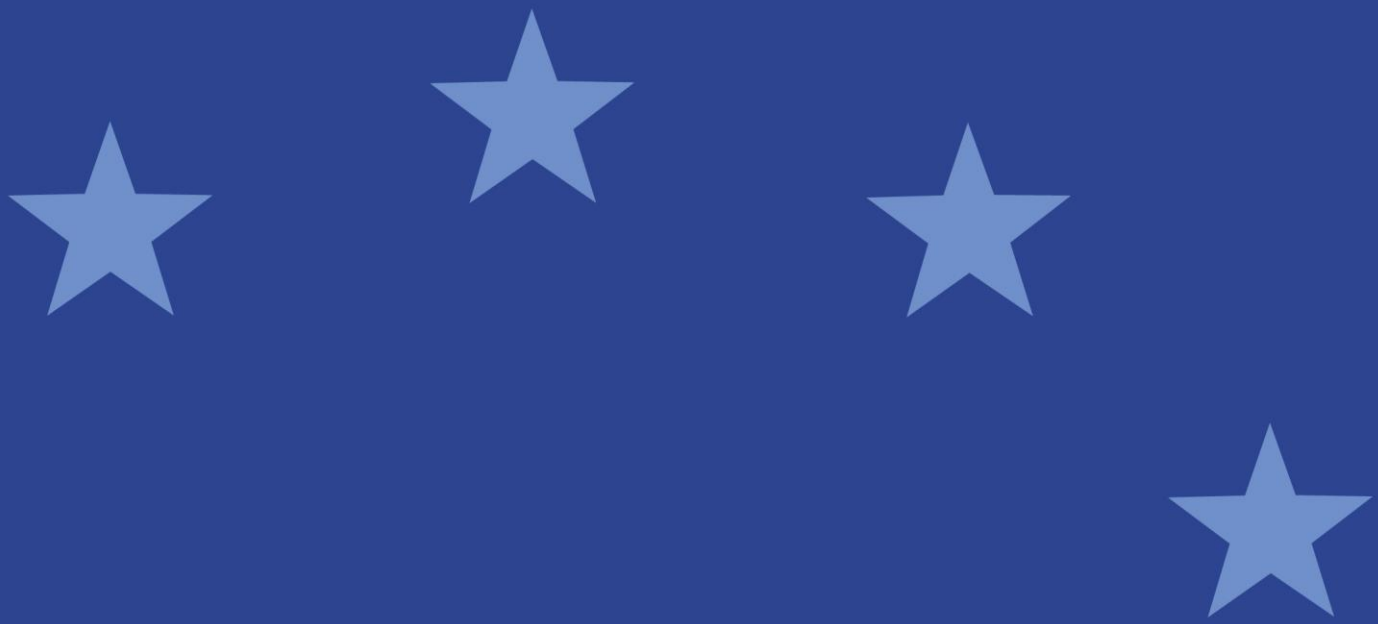
esma European Securities and Markets Authority

Final Report

Guidelines on outsourcing to cloud service providers



18 December 2020 | ESMA50-157-2403

Table of Contents

I. Executive Summary

Reasons for publication

The increasing use of outsourcing to cloud service providers by firms brings benefits but is not exempt of challenges and risks.

The purpose of the guidelines is to help firms identify, address and monitor the risks that may arise from their cloud outsourcing arrangements and to support a convergent approach to the supervision of cloud outsourcing arrangements across competent authorities in the EU.

Bearing in mind that the main risks associated with cloud outsourcing are similar across sectors, ESMA has considered the EBA Guidelines on outsourcing arrangements[1], which have incorporated the EBA Recommendations on outsourcing to cloud service providers[2], and the EIOPA Guidelines on outsourcing to cloud service providers[3], with a view to ensure consistency between the three sets of guidelines. ESMA is also mindful of the proposal for a Digital Operational Resilience regulation[4] published by the European Commission in September 2020. ESMA will continue to closely monitor the development of this proposal to provide revised or additional guidance as necessary.

On 3 June 2020, ESMA published a Consultation Paper (CP)[5] with proposed draft Guidelines. The consultation period closed on 1 September 2020. ESMA received 48 responses, 7 of which confidential. The answers received are available on ESMA's website, unless respondents requested otherwise.

This Final Report provides an overview of the feedback received through the responses to the CP and explains how ESMA took this feedback into account. It also contains the final set of Guidelines on outsourcing to cloud service providers. ESMA recommends reading this report together with the CP published on 3 June 2020 to have a complete view of the rationale for the guidelines.

Contents

Section II sets out an Overview of the document. Annex I provides the Feedback Statement. Annex II sets out the cost-benefit analysis which details the expected impact of the Guidelines.

The Guidelines are set out in Annex III.

Next Steps

The guidelines in Annex III will be translated in the official EU languages and published on ESMA's website. The publication of the translations in all official languages of the EU will trigger a two-month period during which NCAs must notify ESMA whether they comply or intend to comply with the guidelines.

II. Overview

Background

1. IT outsourcing is a common practice for firms, and cloud computing solutions are increasingly becoming the preferred IT outsourcing option for many firms. While the use of cloud services is a form of IT outsourcing and the general principles regarding effective controls for outsourcing apply, ESMA recognises that certain features are specific to cloud services. Compared with more traditional forms of IT outsourcing, cloud services tend to be more standardised and provided to clients in a highly automated manner and at large scale.

2. ESMA acknowledges that cloud outsourcing can bring benefits, including enhanced flexibility, operational efficiency, and cost effectiveness, with potential positive outcomes for firms and investors. Yet, cloud outsourcing is not exempt of challenges and risks for firms, including in relation to governance, risk assessment and oversight, contractual terms, information security, reliance on providers that may not be easily substitutable and supervision by competent authorities. The guidelines are intended to help firms identify, monitor and mitigate those risks in a relevant manner and to support supervisory convergence in the EU.

3. In accordance with Articles 1(5) and 8(3) of the ESMA Regulation, ESMA has taken into account the principle of proportionality when drafting these guidelines. For example, the guidelines differentiate between critical or important functions and non-critical or important functions, to consider the risk underlying the outsourcing of those functions.

4. Furthermore, ESMA considers that competent authorities should also have regard to the principle of proportionality when supervising compliance with these guidelines, for example by considering the scope and complexity of the outsourced functions, as well as the risks arising from the outsourcing arrangements.

5. These guidelines are without prejudice to applicable requirements in sectoral legislation. They are also without prejudice to more stringent guidelines or supervisory practices applicable to certain categories of firms.[6]

6. It is the responsibility of firms to manage risks in relation to the use of cloud services.

Public consultation

7. On 3 June 2020, ESMA published a Consultation Paper (CP) with proposed draft Guidelines. The consultation period closed on 1 September 2020.

[6] For example, CRAs may satisfy compliance with guideline 8 by complying with the guideline document on 'the submission of periodic information to ESMA by CRAs' and in particular Template 16 thereof.

8. ESMA received 48 responses, 7 of which confidential, from a wide variety of respondents, including representatives of financial institutions, investment firms, financial market infrastructures and cloud service providers. The answers received are available on ESMA's website unless respondents requested otherwise.

9. In general, respondents agree with ESMA's approach towards outsourcing to cloud service providers.

10. The detailed content of the responses and ESMA feedback is outlined in the Feedback Statement.

III. Annexes

Annex I: Feedback Statement

Guideline 1 – Governance, oversight and documentation

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 provisions? Please explain.

11. Respondents were broadly in agreement with ESMA's risk-based approach and focus on critical or important functions. Yet, an elevated number of respondents required further guidance on the definition of key terms, including 'critical or important function', 'cloud service provider' and 'cloud outsourcing arrangement' and several insisted on the need to ensure consistency with EBA's guidelines (the request for consistency with EBA's guidelines was effectively repeated across the board), including with a view to reduce costs and implementation risks. Several respondents suggested to include examples of critical or important functions (or reference definitions in existing regulations) and cloud outsourcing arrangements to foster a convergent approach across firms and competent authorities. The application of the guidelines to situations where the outsourcing to the CSP is intermediated by a non-CSP third party also raised questions, some respondents being of the view that it would be too far-reaching. A few respondents would see merit in including a definition of 'outsourcing'. Several requested clarifications regarding possible interactions with EBA guidelines for entities falling within the scope of both sets of guidelines.

12. Several respondents considered cloud outsourcing as a form of outsourcing and did not see a strong rationale for a standalone approach. They asked for clarification that the cloud outsourcing strategy can form part of existing information security strategies at the firm. Similarly, they requested clarification that existing governance bodies or vendor management processes could perform the oversight and governance functions for cloud outsourcing arrangements. A few respondents requested further guidance on the notion of small and less complex firms, a few others asked ESMA to better consider group structures and one said that the wording of paragraph 27 of the proposed guidelines was ambiguous.

13. Respondents generally agreed with the need for an inventory of cloud outsourcing arrangements but several highlighted that having a single dedicated register for the purpose of the cloud would be burdensome and instead required flexibility from ESMA, including through the clarification that the requested information can be obtained from various sources. Several objected that providing an explanation as to why an outsourced function is considered not important or critical would have little value, and that the focus instead should be on critical or important functions.

14. Several respondents raised comments/questions on the level of information that would need to be provided in relation to sub-outsourcers, considering that CSP tend not to provide that level of details. There were also questions in relation to the location of data, with the reference to countries instead of regions being problematic, and the request to limit location provisions to where data are stored. The inclusion of budget costs was considered by several respondents as of little relevance and some suggested to remove the reference to VAT.

ESMA response:

15. The guidelines already provide a definition of critical or important functions, including criteria to be considered for the assessment of critical or important functions, which is consistent with the MIFID framework and Commission Delegated Regulation (EU) No 2017/565. ESMA does not believe that being more prescriptive would be helpful, also considering the wide range of firms within the scope of the guidelines. For the same reason, we do not believe that a definition of outsourcing or small and less complex firms would be helpful at this level. Meanwhile, ESMA has amended the definition of cloud outsourcing arrangement to clarify those situations where the outsourcing to the CSP is intermediated by a non-CSP third party that would fall within the scope of the guidelines.

16. ESMA has noted the request from some participants to better consider group structures but believes that the current drafting is relevant to firms, including where they are part of a wider group. The background section of the report clarifies that these guidelines are without prejudice to applicable requirements in sectoral legislation. They are also without prejudice to more stringent guidelines or supervisory practices applicable to certain categories of firms.

17. The guidelines are not prescriptive on the exact form that the cloud outsourcing strategy needs to take, meaning that they may form part of broader IT or outsourcing strategies. The same holds true for the governance and oversight framework of cloud outsourcing arrangements.

18. ESMA has clarified in paragraph 14 of the final guidelines (paragraph 27 of the proposed guidelines) that the monitoring of the CSP by the firm should be risk-based, with a primary focus on those cloud outsourcing arrangements that concern critical or important functions.

19. When it comes to the documentation of cloud outsourcing arrangements, ESMA believes that an explanation as to why an outsourced function is or is not considered critical or important is meaningful from a supervisory perspective, also considering the implications for the application of the guidelines. ESMA also believes that the documentation provisions on sub-outsourcers are relevant, considering the risks involved. Meanwhile, ESMA has amended the provision on the location of data to include the reference to regions and focus on where data are stored. ESMA has also removed the reference to VAT for the budget costs. As to the form, it does not matter whether the register is sourced from various data components or a stand-alone data

repository, as long as the information can be provided in an effective and timely manner to the competent authority on request.

20. Importantly, when reflecting on the feedback provided by respondents, ESMA has been careful to ensure consistency with the EBA and EIOPA guidelines. ESMA is also mindful of the proposal for a Regulation on Digital Operational Resilience[7] from the European Commission, bearing in mind that the text is still a proposal at this point, and the IOSCO consultation[8] on new proposed principles on outsourcing.

Guideline 2 – Pre-outsourcing analysis and due diligence

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.

21. Respondents were in broad agreement with ESMA's proposed risk-based approach with regards to the pre-outsourcing analysis and the due diligence to be performed by firms. One respondent only argued that the due diligence and risk assessment should be performed regardless of the criticality of the outsourced function and another that proportionality was irrelevant from a cyber security perspective. Two others raised concerns with regards to the assessment of conflicts of interest, one saying that firms should retain flexibility and the other that the current drafting was open to interpretation. Two other respondents would welcome further guidance from ESMA on how the pre-outsourcing analysis and due diligence should be proportionate to the nature, scale and complexity of the planned outsourced function.

22. Many respondents argued that firms should not be requested to monitor concentration risk at sector level, as they lack the necessary insights to do so and that this should rather fall on competent authorities. The provision on the political stability, the security situation and the legal system (including insolvency law) of the countries where the outsourced functions would be provided and/or data stored was perceived by many as potentially challenging and burdensome. A few respondents wondered why firms should undertake such assessments for EU countries. One highlighted that interoperability and portability could prove challenging and another requested to consider the possibility for firms to re-internalise some of the outsourced functions. One respondent requested to include a reference as to whether the conditions for transfer of personal data to a third country under the GDPR would be met, as this is key to assessing the potential legal risks and compliance issues. Finally, one raised concern on the level of information requested in relation to sub-outsourcing chains.

23. Several respondents found the drafting of paragraph 36 of the proposed guidelines somewhat unclear and insisted that the review of the pre-outsourcing analysis and due diligence should not be set at specified intervals but rather focus on changes in risk

[7] EC, 2020. 'Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector', COM/2020/595 final.
[8] IOSCO, 2020. 'IOSCO consults on new proposed principles on outsourcing', May 2020.

profiles and incidents. Several respondents would also see merit in ESMA providing a list of 'preferred' CSPs or certifications that firms could consider for their risk assessment.

ESMA response

24. ESMA notes the broad support for the proposed approach and believes that the guidelines provide the right level of guidance already when it comes to the due diligence and risk assessment to be performed by firms before entering into cloud outsourcing arrangements.

25. ESMA agrees that national competent authorities are instrumental in monitoring concentration risk at sector level. However, firms should be mindful of the dominant position of certain CSPs when entering into cloud outsourcing arrangements, including because these providers may not be easily substitutable. ESMA recognises the complexity involved in assessing the security situation and legal system of the countries where the outsourced services are likely to be provided and/or data stored. However, ESMA believes that this is an important driver of risks for cloud outsourcing arrangements, which deserves a thorough assessment.

26. ESMA has amended the drafting of paragraph 36 of the proposed guidelines and moved it under Guideline 1, as indeed the assessment of the criticality or importance of an outsourcing function fits better under Guideline 1. ESMA also agreed with the suggestion to consider that outsourced functions may be re-internalised by the firm and included a reference to the transfer of personal data to a third country under GDPR. Providing a list of preferred CSPs or certifications is not something that falls within ESMA's remit.

Guideline 3 – Contractual provisions

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

27. The respondents generally supported the intention of the guideline and agreed that the rights and obligations of a firm and of its CSP should be set out clearly in a written agreement. Yet, many highlighted that CSPs typically provide standardized contracts. Depending on their size and associated bargaining powers, firms may therefore be limited in their ability to negotiate contractual terms.

28. The provision on the location of data was widely commented. Some respondents highlighted the dynamic nature of data processing, and hence the challenges involved in notifying location changes. Others mentioned possible interactions/overlaps with GDPR and requested clarification as to whether paragraph 41(g) of the proposed guidelines was aimed at personal data or data in general.

29. Some respondents requested more guidance on the right for firms to monitor the performance of their CSP, e.g., in terms of frequency or scope, when others highlighted

the possible limitations imposed by CSPs. Two respondents said that precise quantitative and qualitative targets were not always available or relevant. Some respondents requested more proportionality regarding the management of incidents.

30. Many respondents underlined that firms are often not able to impose contract terms that would allow them to audit the books, premises and devices of their CSPs. One respondent said access and audit rights of firms should be unrestricted. However, others argued that unlimited access to the premises and systems of the CSPs would create risks and suggested instead that firms rely on third-party certifications or audits. Some also requested greater clarity on the exercise of access and audit rights by competent authorities.

31. Some respondents were concerned that the term 'written agreement' implied a single document, where several documents may exist in practice. Other respondents flagged that termination was effectively limited to a set of specific situations. Finally, some respondents recommended that ESMA, together with EBA and EIOPA, develop standard contractual clauses, which could be adopted by providers and firms on a voluntary basis.

ESMA response:

32. ESMA is cognisant of the fact that firms, including smaller ones, often face challenges to impose bespoke contractual terms on their CSPs. Yet, ESMA believes that the rights and obligations of the firms and their CSPs should to be set out clearly and extensively in a written agreement (which may effectively take the form of a single or several documents). This guideline, by setting detailed provisions in that respect, is also intended to help firms negotiate contractual terms with their CSPs.

33. Consistent with EBA's and EIOPA's guidelines, ESMA believes that the location where relevant data may be stored and processed is important from a risk management perspective and therefore needs to be set out in a written agreement. In respect of personal data, the definition of "processing" in Article 4(2) of GDPR applies.[9] ESMA has clarified that regions or countries (instead of countries only) are relevant for the location of data. Paragraph 41 (g) of the proposed guidelines (paragraph 28 (g) of the final guidelines) covers the protection of personal data and other types of data through the term 'information security' having regard to guideline 4.

34. ESMA has cross-referenced guideline 6 to provide more background in terms of expectations for the monitoring of CSP performance. ESMA has also clarified the provision on incident management.

35. Finally, ESMA agrees with the view that standard contractual clauses may prove beneficial and looks forward to the work that the Commission has undertaken on the topic.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Guideline 4 – Information security

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

36. Many respondents were of the view that the proposed drafting was overly prescriptive and not reflective enough of the different types of cloud outsourcing models. They requested a more principle-based approach and asked ESMA to remove some of the provided examples, as they were not always illustrative of best practices and/or might become obsolete as the technology continues to evolve quickly. Several respondents highlighted that firms should remain in control of the decision to outsource or not the storage and management of encryption keys to their CSPs and that two-factor authentication was not necessarily the best solution across all areas. One observed that market solutions in relation to data in memory were not mature enough yet. Another observed that mechanisms to integrate cloud services with the systems of the firm were good practice, with the downside though that they could increase the firm's dependency on the CSP. There were also some requests for more proportionality, including in respect of smaller firms.

37. Another general comment was that greater alignment with other initiatives on ICT security, e.g., the NIS Directive, and GDPR and the EBA guidelines would be welcome. Two respondents felt that ESMA's approach to the cloud was more conservative than EBA and EIOPA. One respondent said that it could be useful to specifically refer to the international standards that the CSP would be required to apply.

ESMA response:

38. Consistent with EBA and EIOPA, ESMA has a balanced approach to the cloud, meaning that while ESMA is cognizant of the benefits that it can bring to firms, we are mindful of its risks as well. The provisions on information security have been drafted with due consideration to the requirements introduced by the NIS Directive and build on European and internationally recognized technical standards and industry best practices, such as the ISO 27000 standards, ENISA's cloud assurance framework NIST standards and the Cloud Security Alliance initiative. They also leverage on ESMA and competent authorities' supervisory experience.

39. The provided examples are not meant to be exhaustive. Rather, they are intended to help firms better understand the provisions of the guideline and identify and put in place relevant mitigants for the wide variety of information security risks that may arise as a result of their cloud outsourcing arrangements. ESMA recognizes that cloud computing and information security solutions and paradigms are evolving rapidly. The provisions are therefore organized around key principles. Meanwhile, ESMA has reviewed some of the examples considering the different business models and the evolving nature of the technology.

40. ESMA has also clarified that the information security requirements set by the firm should be proportionate to the nature, scale and complexity of the function that the firm

outsources to the CSP and the risks inherent to this function. Meanwhile, firms should include information security requirements in their internal policies and outsourcing agreements and monitor compliance with those requirements, having also regard to all the legal requirements regarding the protection of data that apply to the firm (e.g. protection of personal data and secrecy or similar legal confidentiality duties with respect to clients' information). Firms should verify that CSPs have in place appropriate controls for information security, including in particular for the protection of confidential, personal or otherwise sensitive data.

Guideline 5 – Exit strategies

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

41. Respondents agreed on the need of having a clearly defined exit strategy to ensure the possibility to discontinue cloud outsourcing agreements without undue disruption of business activities and/or services to clients, nor detriment to compliance with legal requirements, confidentiality and integrity, in case there are critical or important functions involved.

42. A significant number of respondents commented on the testing of exit strategies. Several highlighted that full testing was not practical and that firms should not be expected to have fully 'implemented' exit plans. Others requested further guidance on the frequency of testing. Several insisted on the need to have a risk-based approach and to account for differences in the scope and type of cloud arrangements and types of exits.

43. The transfer and/or removal of data attracted various comments. Several respondents highlighted that the firm, and not the CSP, would be in control of these operations under certain cloud outsourcing arrangements. Yet, the CSP should always enable and support the transfer and/or removal of data in case the firm activates the exit strategy. Some respondents also requested more guidance on the way in which a firm should ensure that its data have been effectively removed from the CSP and suggested to rephrase the guideline to instead highlight the obligation by the CSP to delete the data removed or transferred. One requested clarification that cryptographic deletion would suffice. Other respondents said that the applicable provisions should be consistent with GDPR.

44. Finally, some commented that the guidelines assume that there is a possibility to have a customized contract with a CSP, which is not necessarily the case as the bargaining power of smaller firms may be limited.

ESMA response:

45. ESMA has amended the guideline and provided additional guidance in respect to the testing of exit strategy, as indeed 'full' testing may not be practical for firms.

46. ESMA has also amended the guideline to clarify that the CSP should support the orderly transfer of the outsourced functions and the related processing of data, including where relevant its secure deletion from the systems of the CSP.

47. ESMA does not believe that further guidance on the frequency of testing or practical means to ensure the deletion of data would add value, considering the different business models and possible risks involved. Also, the provisions on data are without prejudice to the possible application of GDPR. Comments on the fact that firms may have a limited leeway to negotiate contractual terms with CSPs are addressed under Guideline 3.

Guideline 6 – Access and audit rights

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

48. This guideline was widely commented, which is understandable considering the importance of access and audit rights from a risk management perspective and the dissenting views that prevail between firms and their CSPs on the topic. The comments were mainly twofold:

49. First, many firms observed that they often lack the necessary bargaining power to impose extensive access and audit rights on their CSPs. Because there are few alternatives, CSPs tend to impose their conditions on firms. In particular, on-site access is typically not allowed. A handful of respondents also highlighted the costs involved in extensive audits and the operational and security risks they could raise at CSPs. Against this background, the use of third-party certifications and audit reports is generally seen as a reasonable approach, although several respondents insisted on the need to clarify that the cloud outsourcing arrangement should not limit the access and audit rights of firms. Several respondents also suggested to include a carveout to ensure that alternative methods are only used in case the exercise of access or audit rights create tangible risks to the CSP or its clients.

50. Second, respondents raised a series of practical questions/comments on the use of third-party certifications and audit reports. Some said that it would be challenging to assess the relevance of third-party certifications, including in terms of scope, contents or expertise of staff undertaking the work, as it would require knowledge and resources that are not always available at firms, including smaller ones. Some suggested that providing a list of relevant certifications might be helpful. A handful of respondents wondered whether the use of third-party certifications and audit reports could make access and audit rights redundant.

51. The “right to request the expansion of the scope of certifications or audit reports” is a contentious point. Most firms do not question its relevance but see challenges in imposing such provisions to large CSPs. Other respondents argued that third-party certifications and audit reports are standard by design and cover the needs of as many

customers as possible, reducing the burden of individual assessments. Several respondents also raised questions in relation to pooled audits, questioning their relevance from a practical perspective.

52. Other comments included the suggestion to clarify that (i) paragraph 52 of the proposed guidelines applies to critical or important functions and (ii) in paragraph 53, the prior notice would not apply either in case the notice of audit would make such audit no longer effective.

ESMA response:

53. Extensive access and audit rights are instrumental to firms to ensure that the CSP delivers on its services and that risks are properly managed. ESMA believes that the guidelines strike the balance right between the need to protect these access and audit rights and at the same time remain proportionate, not to impose provisions that would put an excessive burden on firms and CSPs with very limited tangible benefits. ESMA agreed with the suggestion to highlight that CSPs should substantiate the reason why the use of access and audit rights create risks to them or their clients and therefore warrant the use of alternative methods to be agreed with the firm, with a view to empower firms with their rights.

54. ESMA believes that the use of third-party certifications and audit reports is relevant under certain conditions only. A firm should assess such certifications and reports regularly and thoroughly, to ensure that they are adequate in terms of scope, relevant and performed according to best standards and practices. Furthermore, the use of such certifications and audit should not be interpreted as limiting the right of a firm to perform on-side audits at its discretion. ESMA has also clarified that firms should aim not to rely exclusively on such third-party certifications and audits over time. ESMA introduced an additional element of proportionality with regards to requests for expansion of the scope of certifications or audit reports, as indeed ESMA believes that these requests should remain proportionate. ESMA also reflected the clarifications requested in paragraphs 52 and 53 of the proposed guidelines.

Guideline 7 – Sub-outsourcing

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

55. Several respondents wondered whether this guideline intended to capture the sub-outsourcing of non-material parts of critical or important functions, which they would see, except for one of them, as disproportionate. One respondent requested further clarity on the exact definition of sub-outsourcing and another on the way in which sub-outsourcing chains would need to be considered.

56. Several respondents insisted on the need to underline that CSPs should retain full responsibility and accountability in case of sub-outsourcing and some said that it would

be challenging for firms to ensure that their CSPs effectively oversee the sub-outsourced functions. Others suggested to highlight, like in the EBA and EIOPA guidelines, that the conditions for sub-outsourcing should include the assurance that the sub-outsourcing provider complies with the applicable rules and the contractual requirements set between the firm and the CSP.

57. Several respondents highlighted that notification details are typically set by the CSPs and not negotiable. Others found the notification provision excessively burdensome and suggested to apply it only in cases where sub-outsourcing might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement. Others requested further guidance on the meaning of 'material change', 'sufficient notification period' and 'duration of a risk assessment'. Several respondents insisted on the need to set long enough notification periods so that a proper risk assessment may be conducted prior to the planned sub-outsourcing.

58. Several respondents said that the right to object raised practical challenges, some arguing that such right would be damaging to the quality of the services provided. A few respondents commented on undue sub-outsourcing, one saying that the drafting was too restrictive and another that it was all-encompassing. Finally, some respondents requested further clarity in relation to intra-group outsourcing agreements.

ESMA response:

59. ESMA has clarified that the guideline applies to the sub-outsourcing of critical or important functions, or 'material' parts thereof. The definition section of the guidelines includes a definition of sub-outsourcing.

60. ESMA has emphasized that CSPs should retain full accountability for those services that they sub-outsource, as indeed we believe that this is an important point that needs to be spelled out. This is without prejudice to the final responsibility of firms, which remain fully responsible for their outsourced functions.

61. ESMA believes that the obligation for CSPs to notify firms of any planned outsourcing and the right for firms to object to such sub-outsourcing are important safeguards. ESMA has further specified that the notification period should be long enough at least for firms to carry out a risk assessment and to object or approve the sub-outsourcing. Finally, the need to distinguish between intra-group and other types of sub-outsourcing is not obvious to ESMA, considering the similar risks involved.

Guideline 8 – Written notification to competent authorities

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

62. Respondents see value in notification provisions where there are critical or important functions involved, with a view to help competent authorities assess risks stemming from cloud outsourcing arrangements both at individual firm and industry level.

63. Several respondents requested clarifications in relation to the notification process. Some raised concerns that the notification might be interpreted as pre-approval by competent authorities. Some argued that a more precise time frame and reporting templates would be useful, to foster consistency across firms and competent authorities. Several suggested to notify competent authorities only after the outsourcing arrangement has been signed, as the required information may not always be available prior to that. Another respondent suggested to apply the notification provisions at an overall relationship level, not when additional services are onboarded to the same CSP.

64. Several respondents questioned the breadth of information to be included in the notification. Consistent with guideline 1, some expressed concerns on the need to specify where the data are processed and asked to include a reference to regions and not only countries. Some questioned the relevance of including the date of the most recent criticality assessment and the date of last risk assessment and requested further alignment with EBA guidelines.

65. Finally, several respondents highlighted some overlaps with existing notification provisions at sectoral level and some suggested not to require firms to separately notify their competent authority of CSP outsourcing, if that notification is already covered by other specific legislation.

ESMA response:

66. ESMA believes that the drafting of the guideline is precise enough, including on the need for firms to be timely in their notification of planned cloud outsourcing arrangements. When it comes to the contents of the notification provisions, ESMA has amended the drafting of several provisions, for consistency purposes with the documentation provisions under Guideline 1.

67. As highlighted in the background section, these guidelines are without prejudice to applicable requirements in sectoral legislation. They are also without prejudice to more stringent guidelines or supervisory practices applicable to certain categories of firms. For Credit Rating Agencies that are supervised by ESMA, the notification under Guideline 8 should be considered as being satisfied through the CRAs compliance with Item 36 of ESMA's Guidelines on Periodic Information Submitted by Credit Rating Agencies[10].

Guideline 9 – Supervision of cloud outsourcing arrangements

[10] Guidelines on the submission of periodic information to ESMA by Credit Rating Agencies – 2nd Edition

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

68. Most respondents agreed with the suggested approach, in particular as it would allow competent authorities to monitor CSP concentration risk. Several respondents highlighted that they would see value in competent authorities reporting back on concentration risks to promote greater visibility and understanding of concentration risk to firms.

69. Some would welcome further guidance with a view to foster greater convergence in terms of supervisory and reporting practices by competent authorities in the EU. Several respondents required clarifications in support of a centralised approach for cross-border groups, also to avoid duplicate efforts by NCAs.

ESMA response:

70. ESMA notes that some respondents would see value in competent authorities reporting on concentration risk and greater harmonisation across Member States, which is something that may be explored further in the context of DORA.

Additional feedback

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.

71. Many respondents reiterated the comments/questions that they raised under Guideline 1 in relation to the definition of key terms and consistency with EBA's and EIOPA's guidelines. Some respondents also raised targeted questions on the exact scope of the guidelines, in relation to UCITS, non-EU CCPs and third-country benchmarks administrators. One suggested to exempt providers of global financial messaging services subject to oversight from the guidelines. Finally, some respondents commented on the implementation timeline of the guidelines, one requesting that the time to comply be extended and others that existing arrangements be exempted from the pre-outsourcing analysis.

72. Only a handful of respondents provided some indications on the resources that would be needed to implement and comply with the guidelines. One estimated the cost to comply with ESMA's guidelines to be around EUR 0.5m (not including extra charges by suppliers who charge for contract adaptations). Another said that 5-6 senior

engineers would be needed. Several highlighted the significant resources necessary to test exit strategies, if the provision to test exit strategy was to be interpreted extensively. Many respondents said that they were not able to provide estimates, including because several provisions of the guidelines required further clarification. Several others highlighted that they were mostly compliant with the guidelines already, and therefore expected to leverage on existing resources to a large extent. Finally, several respondents highlighted that costs would be significantly reduced by aligning further the guidelines with EBA and EIOPA guidelines.

ESMA response:

73. The comments regarding the definition of key terms and interactions with EBA's and EIOPA's guidelines have been addressed under Guideline 1. The exact scope of the guidelines is set out in section 1.1. As far as the firms referred to in points (i) and (ii) of the Scope - Section 'Who?' - are concerned, these Guidelines apply insofar as a cloud service arrangement entered into by those firms qualifies as a delegation arrangement under the UCITS and AIFM regulatory frameworks.

74. ESMA has removed third-country benchmark administrators from the scope of the guidelines, for consistency purposes with the DORA proposal. ESMA does not believe that explicitly exempting global financial messaging services from the ESMA guidelines is necessary, as the guidelines focus on cloud outsourcing and not outsourcing in general, like the EBA guidelines.

75. ESMA has extended by a month the application date of the guidelines.

Annex II: Cost-benefit analysis

Introduction

76. Firms are increasingly outsourcing to CSPs. Cloud outsourcing can bring benefits to firms, and in turn investors, through reduced costs and enhanced operational efficiency and flexibility. Yet, the use of cloud services raises a series of challenges in terms of data protection and location, security issues and concentration risk, which may translate into important risks to investor protection, market integrity and financial stability, if not appropriately addressed.

Impact of the ESMA guidelines

77. Considering the main objectives of these guidelines, we set out below a preliminary assessment of the expected benefits and costs of the guidelines.

Benefits

78. ESMA believes the main benefits linked to the introduction of the guidelines are to:

    a) support firms in their prudent transition to the cloud, by providing clarity on the applicable regulatory provisions and supervisory expectations, and help unlock the benefits that this technology provides to firms and ultimately investors;

    b) provide a framework for cloud outsourcing that is consistent across sectors, and allow for economies of scale for firms and CSPs with regards to compliance costs;

    c) reduce the risks of arbitrage through enhanced regulatory and supervisory convergence across competent authorities;

    d) maximise the investments made by competent authorities to supervise cloud outsourcing arrangements, e.g. skills and resources, including where they have cross-sectoral mandates;

    e) reduce the risks in relation to the use of cloud services and their potential negative outcomes.

Costs

79. As a preliminary note, it is reasonable to expect that those firms that already have a complete set of arrangements in place to comply with the existing general frameworks on outsourcing, will incur fewer overall costs when implementing these guidelines. Several respondents to the public consultation reported that they were already broadly in compliance with the provisions in the guidelines.

80. ESMA considers that potential and incremental costs that firms will face when complying with these guidelines might be of a one-off and / or ongoing nature, arguably linked to:

    a) (direct) costs linked to the update/review of the existing procedural and organisational arrangements, including the implementation and maintenance of a formal register of cloud outsourcing arrangements;

b) (direct) initial and ongoing IT costs;

c) (direct) relevant organisational and HR costs linked to the implementation of the guidelines, including in relation to the risk assessment, due diligence and oversight of the cloud service providers;

81. ESMA believes that the proposed option provide the most cost-efficient solution to achieving the general objectives of these guidelines.

Conclusions

82. In light of the above, the overall impact on firms is considered low. The guidelines set out a limited set of provisions, with a focus on those cloud outsourcing arrangements that concern critical and important functions. In addition, ESMA expects competent authorities to adopt a risk-based approach when supervising compliance with these guidelines, including with a view to mitigate implementation costs for smaller firms.

83. ESMA believes that the overall (compliance) costs associated with the implementation of the guidelines will be compensated by the benefits arising from the enhanced regulatory certainty and risk management framework. These benefits will interest all firms under the scope of the guidelines.

84. ESMA also considers that the guidelines support greater harmonisation in the interpretation and consistent application of the provisions listed in Section 1.1 under the heading 'What?' of the guidelines (see Appendix III) across Member States in the case of cloud outsourcing, thereby minimising the potential adverse impact linked to compliance costs. These benefits will outweigh all associated costs in respect of these guidelines.

85. Finally, ESMA believes that the adoption of the guidelines is the best tool to provide clear guidance to firms on how to enter cloud outsourcing arrangements with CSPs. Furthermore, the adoption of guidelines further reduces the risk of diverging interpretations that might lead to discrepancies in the application and supervision of the relevant provisions across Member States (determining a risk of regulatory arbitrage and circumvention of rules). ESMA has also be mindful to ensure consistency with EBA's and EIOPA's guidelines to provide for economies of scale at firms, CSPs and competent authorities.

Annex III: Guidelines on Outsourcing to Cloud Service Providers

1.1. Scope

Who?

1. These guidelines apply to competent authorities and to (i) alternative investment fund managers (AIFMs) and depositaries of alternative investment funds (AIFs), (ii) undertakings for collective investment in transferable securities (UCITS), management companies and depositaries of UCITS, and investment companies that have not designated a management company authorised pursuant to UCITS Directive (iii) central counterparties (CCPs), including Tier 2 third-country CCPs which comply with the relevant EMIR requirements, (iv) trade repositories (TRs), (v) investment firms and credit institutions when carrying out investment services and activities, data reporting services providers and market operators of trading venues, (vi) central securities depositories (CSDs), (vii) credit rating agencies (CRAs), (viii) securitisation repositories (SRs), and (ix) administrators of critical benchmarks.

2. ESMA will also take these guidelines into account when assessing the extent to which compliance with the relevant EMIR requirements by a Tier 2 third-country CCP is satisfied by its compliance with comparable requirements in the third country pursuant to Article 25(2b)(a) of EMIR.

What?

3. These guidelines apply in relation to the following provisions:

   a) Articles 15, 18, 20 and 21(8) of AIFMD; Articles 13, 22, 38, 39, 40, 44, 45, 57(1)(d), 57(2), 57(3), 58, 75, 76, 77, 79, 81, 82 and 98 of Commission Delegated Regulation (EU) 2013/231;
   b) Articles 12(1)(a), 13, 14(1)(c), 22, 22a, 23(2), 30 and 31 of UCITS Directive; Article Articles 4(1) to 4(3), 4(5), 5(2), 7, 9, 23(4), 32, 38, 39 and 40 of Commission Directive 2010/43/EU; Articles 2(2)(j), 3(1), 13(2), 15, 16 and 22 of Commission Delegated Regulation (EU) No 2016/438;
   c) Articles 25, 26(1), 26(3), 26(6), 34, 35 and 78-81 of EMIR; Articles 5 and 12 of SFTR; Articles 3(1)(f), 3(2), 4, 7(2)(d) and (f), 9 and 17 of Commission Delegated Regulation (EU) No 153/2013; Articles 16 and 21 of Commission Delegated Regulation (EU) No 150/2013; Articles 16 and 21 of Commission Delegated Regulation (EU) 2019/359;
   d) Articles 16(2), 16(4), 16(5), 18(1), 19(3)(a), 47(1)(b) and (c), 48(1), 64(4), 65(5) and 66(3)11 of MiFID II; Articles 21(1) to (3), 23, 29(5), 30, 31 and 32 of Commission Delegated Regulation (EU) No 2017/565; Articles 6, 15 and 16 (6) of Commission Delegated Regulation (EU) No 2017/584; Articles 6, 7, 8 and 9 of Commission Delegated Regulation (EU) No 2017/571;

[11] As of 1 January 2022, the reference to Articles 64(4), 65(5) and 66(3) of MiFID II should be read as referring to Articles 27g(4), 27h(5) and 27i(3) of MiFIR.

e) Articles 22, 26, 30, 42, 44 and 45 of CSDR and Articles 33, 47, 50 (1), 57(2)(i), 66, 68, 75, 76, 78 and 80 of Commission Delegated Regulation (EU) No 2017/392;
f) Article 9 and Annex I, Section A points 4 and 8 and Annex II point 17 of CRA Regulation and Articles 11 and 25 of the Commission Delegated Regulation (EU) No 2012/449;
g) Article10(2) of SECR;
h) Articles 6(3) and 10 of the Benchmarks Regulation and Point 7 of Annex I of Commission Delegated Regulation (EU) 2018/1646.

When?

4. These guidelines apply from 31 July 2021 to all cloud outsourcing arrangements entered into, renewed or amended on or after this date. Firms should review and amend accordingly existing cloud outsourcing arrangements with a view to ensuring that they take into account these guidelines by 31 December 2022. Where the review of cloud outsourcing arrangements of critical or important functions is not finalised by 31 December 2022, firms should inform their competent authority of this fact, including the measures planned to complete the review or the possible exit strategy.

1.2. Legislative references, abbreviations and definitions

Legislative references

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[12]
AIFMD	Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010[13]
Commission Delegated Regulation (EU) 2013/231	Commission Delegated Regulation (EU) 2013/231 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision[14]
UCITS Directive	Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to

[12] OJ L 331, 15.12.2010, p. 84
[13] OJ L 174, 1.7.2011, p. 1.
[14] OJ L 83, 22.3.2013, p. 1

	undertakings for collective investment in transferable securities (UCITS)[15]
Commission Directive 2010/43/EU	Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company[16]
Commission Delegated Regulation (EU) No 2016/438	Commission Delegated Regulation (EU) 2016/438 of 17 December 2015 supplementing Directive 2009/65/EC of the European Parliament and of the Council with regard to obligations of depositaries[17]
EMIR	Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories[18]
SFTR	Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012[19]
Commission Delegated Regulation (EU) No 153/2013	Commission Delegated Regulation (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties[20]
Commission Delegated Regulation (EU) No 150/2013	Commission Delegated Regulation (EU) No 150/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories with regard to regulatory technical standards specifying the details of the application for registration as a trade repository[21]
Commission Delegated Regulation (EU) 2019/359	Commission Delegated Regulation (EU) 2019/359 of 13 December 2018 supplementing Regulation (EU) 2015/2365 of the European Parliament and of the Council with regard to regulatory technical standards specifying the details of the

[15] OJ L 302, 17.11.2009, p. 32
[16] OJ L 176, 10.7.2010, p. 42
[17] OJ L 78, 24.3.2016, p. 11
[18] OJ L 201, 27.7.2012, p. 1
[19] OJ L 337, 23.12.2015, p. 1
[20] OJ L 52, 23.2.2013, p. 41
[21] OJ L 52, 23.2.2013, p. 25

	application for registration and extension of registration as a trade repository[22]
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU[23]
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 ([24])
Commission Delegated Regulation (EU) No 2017/565	Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive[25]
Commission Delegated Regulation (EU) No 2017/584	Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues[26]
Commission Delegated Regulation (EU) No 2017/571	Commission Delegated Regulation (EU) 2017/571 of 2 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers[27]
CSDR	Regulation (EU) No 909/2014 of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012[28]
Commission Delegated Regulation (EU) No 2017/392	Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories[29]

[22] OJ L 81, 22.3.2019, p. 45
[23] OJ L 173, 12.6.2014, p. 349
[24] OJ L 173, 12.6.2014, p. 84
[25] OJ L 87, 31.3.2017, p. 1
[26] OJ L 87, 31.3.2017, p. 350
[27] OJ L 87, 31.3.2017, p. 126
[28] OJ L 257, 28.8.2014, p. 1.
[29] OJ L 65, 10.3.2017, p. 48

CRA Regulation	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies[30]
Commission Delegated Regulation (EU) No 2012/449	Commission Delegated Regulation (EU) No 449/2012 of 21 March 2012 supplementing Regulation (EC) No 1060/2009 of the European Parliament and of the Council with regard to regulatory technical standards on information for registration and certification of credit rating agencies[31]
SECR	Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012[32]
Benchmark Regulation	Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014[33]
Commission Delegated Regulation (EU) 2018/1646	Commission Delegated Regulation (EU) 2018/1646 of 13 July 2018 supplementing Regulation (EU) 2016/1011 of the European Parliament and of the Council with regard to regulatory technical standards for the information to be provided in an application for authorisation and in an application for registration[34]
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC[35]

Abbreviations

CSP	Cloud service provider
ESMA	European Securities and Markets Authority

[30] OJ L 302, 17.11.2009, p. 1.
[31] OJ L 140, 30.5.2012, p. 32
[32] OJ L 347, 28.12.2017, p. 35.
[33] OJ L 171, 29.6.2016, p. 1
[34] OJ L 274, 5.11.2018, p. 43
[35] OJ L 119, 4.5.2016, p.1-88

EU	European Union

Definitions

function	means any processes, services or activities;
critical or important function	means any function whose defect or failure in its performance would materially impair: a) a firm's compliance with its obligations under the applicable legislation; b) a firm's financial performance; or c) the soundness or the continuity of a firm's main services and activities;
cloud services	means services provided using cloud computing;
cloud computing or cloud[36]	means a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources (for example servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning and administration on-demand;
cloud service provider	means a third-party delivering cloud services under a cloud outsourcing arrangement;
cloud outsourcing arrangement	means an arrangement of any form, including delegation arrangements, between: (i) a firm and a CSP by which that CSP performs a function that would otherwise be undertaken by the firm itself; or (ii) a firm and a third-party which is not a CSP, but which relies significantly on a CSP to perform a function that would otherwise be undertaken by the firm itself. In this case, a reference to a 'CSP' in these guidelines should be read as referring to such third-party.
sub-outsourcing	means a situation where the CSP further transfers the outsourced function (or a part of that function) to another service provider under an outsourcing arrangement;

[36] Cloud computing is often abbreviated into 'cloud'. The term 'cloud' is used throughout the rest of the document for ease of reference.

cloud deployment model	means the way in which cloud may be organised based on the control and sharing of physical or virtual resources. Cloud deployment models include community[37], hybrid[38], private[39] and public[40] clouds;
firms	a) alternative investment fund managers or 'AIFMs' as defined in Article 4(1)(b) of the AIFMD and depositaries as referred to in Article 21(3) of AIFMD ('depositaries of alternative investment funds (AIFs)'); b) management companies as defined in Article 2(1)(b) of the UCITS Directive ("UCITS management companies") and depositaries as defined in Article 2(1)(a) of UCITS Directive ("depositaries of UCITS"); c) central counterparties (CCPs) as defined in Article 2(1) of EMIR and Tier 2 third-country CCPs within the meaning of Article 25(2a) of EMIR which comply with the relevant EMIR requirements pursuant to Article 25(2b)(a) of EMIR; d) trade repositories as defined in Article 2(2) of EMIR and in Article 3(1) of SFTR; e) investment firms as defined in Article 4(1)(1) of MiFID II and credit institutions as defined in Article 4(1)(27) of MiFID II, which carry out investment services and activities within the meaning of Article 4(1)(2) of MiFID II; f) data reporting services providers as defined in Article 4(1)(63) of MiFID II[41]; g) market operators of trading venues within the meaning of Article 4(1)(24) of MiFID II;

[37] A cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection;
[38] A cloud deployment model that uses at least two different cloud deployment models
[39] A cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer
[40] A cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider
[41] As of 1 January 2022, the reference to this provision should be read as a reference to point 36(a) of Article 2(1) of MiFIR.

h) central securities depositories (CSDs) as defined Article 2(1)(1) of CSDR;

i) credit rating agencies as defined in Article 3(1)(b) of the CRA Regulation;

j) securitisation repositories as defined in Article 2(23) of SECR;

k) administrators of critical benchmarks as defined in Article 3(1)(25) of the Benchmarks Regulation.

1.3. Purpose

5. These guidelines are based on Article 16(1) of the ESMA Regulation. The objectives of these guidelines are to establish consistent, efficient and effective supervisory practices within the European System of Financial Supervision (ESFS) and to ensure the common, uniform and consistent application of the requirements referred to in Section 1.1 under the heading 'What?' where firms outsource to CSPs. In particular, these guidelines aim to help firms and competent authorities identify, address and monitor the risks and challenges arising from cloud outsourcing arrangements, from making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities to providing for exit strategies.

1.4. Compliance and reporting obligations

Status of the guidelines

6. In accordance with Article 16(3) of the ESMA Regulation, competent authorities and firms shall make every effort to comply with these guidelines.

7. Competent authorities to which these guidelines apply should comply by incorporating them into their national legal and/or supervisory frameworks as appropriate, including where particular guidelines are directed primarily at firms. In this case, competent authorities should ensure, through their supervision, that firms comply with the guidelines.

8. Through its ongoing direct supervision, ESMA will assess the application of these guidelines by CRAs, TRs, SRs, Tier 2 third-country CCPs and, from 1 January 2022, data reporting services providers and administrators of EU critical benchmarks.

Reporting requirements

9. Within two months of the date of publication of the guidelines on ESMA's website in all EU official languages, competent authorities to which these guidelines apply must notify ESMA whether they (i) comply, (ii) do not comply, but intend to comply, or (iii) do not comply and do not intend to comply with the guidelines.

10. In case of non-compliance, competent authorities must also notify ESMA within two months of the date of publication of the guidelines on ESMA's website in all EU official languages of their reasons for not complying with the guidelines. A template for notifications is available on ESMA's website. Once the template has been filled in, it shall be transmitted to ESMA.

11. Firms are not required to report whether they comply with these guidelines.

1.5. Guidelines on outsourcing to cloud service providers

Guideline 1. Governance, oversight and documentation

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

13. 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 a cloud outsourcing oversight function or designate senior staff members who are 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, including in terms of risk for the financial system, and the risks inherent to the outsourced functions and make sure that their management body has the relevant technical skills to understand the risks involved in cloud outsourcing arrangements[42]. Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and oversight of cloud outsourcing arrangements.

[42] 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).

14. A firm should monitor the performance of activities, the security measures and the adherence to agreed service levels by its CSPs. This monitoring should be risk-based, with a primary focus on the critical or important functions that have been outsourced.

15. A firm should reassess whether its cloud outsourcing arrangements concern a critical or important function periodically and whenever the risk, nature or scale of an outsourced function has materially changed.

16. 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.

17. 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 outsourced function (for example information technology function, control function), which should facilitate the identification of the different types of cloud outsourcing arrangements;
    e) whether the outsourced function supports business operations that are time-critical;
    f) the name and the brand name (if any) of the CSP, its country of registration, its corporate registration number, its legal entity identifier (where available), its registered address, its relevant contact details and the name of its parent company (if any);
    g) the governing law of the cloud outsourcing arrangement and, if any, the choice of jurisdiction;
    h) the type of cloud services and deployment models and the specific nature of the data to be held and the locations (namely regions or countries) where such data may be stored;
    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 of the CSP 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 a critical or important function (or material parts thereof) is sub-outsourced, including the countries where the sub-outsourcers are registered, where the sub-outsourced service will be performed, and the locations (namely regions or countries) where the data will be stored;
m) the estimated annual budget cost of the cloud outsourcing arrangement.

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

Guideline 2. Pre-outsourcing analysis and due diligence

19. 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.

20. The pre-outsourcing analysis and due diligence on the prospective CSP 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.

21. 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 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 or back to the firm;
    vi. the political stability, the security situation and the legal system (including the law enforcement provisions in place, the insolvency law provisions that would apply in case of the CSP's bankruptcy, the laws on data protection in

force and whether the conditions for transfer of personal data to a third country under the GDPR are met) 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 contract 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 EU financial 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 against any significant risks which may arise as a result of the cloud outsourcing arrangement.

22. 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 (including human, IT and financial), the organisational structure and, if applicable, the relevant 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 in particular the protection of personal, confidential or otherwise sensitive data;
    b) the service support, including support plans and contacts, and incident management processes;
    c) the business continuity and disaster recovery plans;

23. 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.

24. If a 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 where needed re-performed.

25. In case a firm enters into a new arrangement or renews an existing arrangement with a CSP that has already been assessed, it should determine, on a risk-based approach, whether a new due diligence is needed.

Guideline 3. Key contractual elements

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

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

28. In case of outsourcing of critical or important functions, the written agreement should include 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 firm's and the CSP's financial obligations;

    e) whether sub-outsourcing is permitted, and, if so, under which conditions, having regard to Guideline 7;

    f) the location(s) (namely regions or countries) where the outsourced function will be provided and where data will be processed and stored, 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 protection of personal data, having regard to Guideline 4;

    h) the right for the firm to monitor the CSP's performance under the cloud outsourcing arrangement on a regular basis, having regard to Guideline 6;

    i) the agreed service levels, which should include, 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 to the firm without undue delay incidents that have affected the operation of the firm's contracted service;

    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 relevant information, premises, 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 that the CSP processes or stores on behalf of the firm can be accessed, recovered and returned to the firm as needed, having regard to Guideline 5.

Guideline 4. Information security

29. 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. These requirements should be proportionate to the nature, scale and complexity of the function that the firm outsources to the CSP and the risks inherent to this function.

30. For that purpose, in case of outsourcing of critical or important functions, and without prejudice to the applicable requirements under GDPR, 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) *identity and access management*: ensure that strong authentication mechanisms (for example multi-factor authentication) and access controls are in place with a view to prevent unauthorised access to the firm's data and back-end cloud resources;
c) *encryption and key management:* ensure that relevant encryption technologies are used, where necessary, for data in transit, data in memory, data at rest and data back-ups, in combination with appropriate key management solutions to limit the risk of non-authorised access to the encryption keys; in particular, the firm should consider state-of-the-art technology and processes when selecting its key management solution;
d) *operations and network security:* consider appropriate levels of network availability, network segregation (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, with the capability to switch from one to the other, or requesting and reviewing documentation showing the transport route of the firm's data among the CSP's systems, as well as considering the possibility to replicate machine images to an independent storage location, which is sufficiently isolated from the network or taken offline);

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

h) *compliance & monitoring*: verify 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).

Guideline 5. Exit strategies

31. In case of outsourcing of critical or important functions, a firm should ensure that it is able to exit the cloud outsourcing arrangement without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with its obligations under the applicable legislation, as well as the confidentiality, integrity and availability of its data. For that purpose, a firm should:

    a) develop 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 transition phase;

    c) ensure that the cloud outsourcing written agreement includes an obligation for the CSP to support the orderly transfer of the outsourced function, and the related processing of 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. The obligation to support the orderly transfer of the outsourced function, and the related treatment of data, should include where relevant the secure deletion of the data from the systems of the CSP and any sub-outsourcer.

32. 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 appropriateness of the exit strategy, using a risk-based approach, (for example, by carrying out an analysis of the potential costs, impact, resources and timing implications of transferring an outsourced service to an alternative provider);
f) define success criteria of the transition.

33. A 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 under the cloud outsourcing arrangement.

Guideline 6. Access and Audit Rights

34. A firm should ensure that the cloud outsourcing written agreement does not limit the firm's and competent authority's effective exercise of the access and audit rights and oversight options on the CSP.

35. 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.

36. 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 CSP should provide a clear rationale to the firm as to why this would create a risk and the CSP should agree with the firm on alternative ways to achieve a similar result (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the CSP).

37. 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.

38. In case of outsourcing of critical or important functions, a firm should assess whether the third-party certifications and external or internal audit reports referred to in

paragraph 37(a) are adequate and sufficient to comply with its obligations under the applicable legislation and should aim at not solely relying on these certifications and reports over time.

39. 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 37(a) only if it:

    a) is satisfied that the scope of the certifications or the audit reports covers the CSP's key systems (for example processes, applications, infrastructure, data centres), the key controls identified by the firm and the compliance with the relevant applicable legislation;
    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 certifications or audit reports;
    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; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective;
    g) retains the contractual right to perform individual on-site audits at its discretion with regard to the outsourced function.

40. A firm should ensure that, before an 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 or would lead to a situation where the audit would no longer be effective. Such notice should include the location, purpose of the visit and the personnel that will participate to the visit.

41. Considering that cloud services 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 auditors acting on its behalf – should have the right skills and knowledge to properly assess the relevant cloud services and perform effective and relevant audit. This should also apply to the firms' staff reviewing the certifications or audit reports provided by the CSP.

Guideline 7. Sub-outsourcing

42. If sub-outsourcing of critical or important functions (or material parts 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 remains accountable and 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 intended 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 set in the written agreement should allow the firm sufficient time at least 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 (for example 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).

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

Guideline 8. Written notification to competent authorities

44. The firm should notify in writing its competent authority in a timely manner of planned cloud outsourcing arrangements that concern a critical or important function. The firm should also notify in a timely manner and in writing its competent authority of those cloud outsourcing arrangements that concern a function that was previously classified as non-critical or non-important and then became critical or important.

45. The firm's written notification should include, taking into account the principle of proportionality, at least the following information:

    a) 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;
    b) a brief description of the outsourced function;

c) a brief summary of the reasons why the outsourced function is considered critical or important;
d) the name and the brand name (if any) of the CSP, its country of registration, its corporate registration number, its legal entity identifier (where available), its registered address, its relevant contact details, and the name of its parent company (if any);
e) the governing law of the cloud outsourcing agreement and, if any, the choice of jurisdiction;
f) the cloud deployment models and the specific nature of the data to be held by the CSP and the locations (namely regions or countries) where such data will be stored;
g) the date of the most recent assessment of the criticality or importance of the outsourced function;
h) the date of the most recent risk assessment or audit of the CSP together with a brief summary of the main results, and the date of the next planned risk assessment or audit;
i) the individual or decision-making body in the firm that approved the cloud outsourcing arrangement;
j) 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, and where the data will be stored;

Guideline 9. Supervision of cloud outsourcing arrangements

46. 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.

47. 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.

48. 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.

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