esma European Securities and Markets Authority

Consultation Paper

Draft Guidelines on Outsourcing to Cloud Service Providers

3 June 2020 | ESMA50-164-3342

Responding to this paper

ESMA invites comments on all matters in this paper and in particular on the specific questions summarised in Appendix 1. Comments are most helpful if they:

- respond to the question stated;
- indicate the specific question to which the comment relates;
- contain a clear rationale; and
- describe any alternatives ESMA should consider.

ESMA will consider all comments received by **1 September 2020**.

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA's Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading 'Data protection'.

Who should read this paper?

This paper is primarily of interest to national competent authorities and financial market participants. In particular, this paper is of interest to alternative investment fund managers, depositaries of alternative investment funds, undertakings for collective investment in transferable securities (UCITS) management companies, depositaries of UCITS, central counterparties, trade repositories, investment firms and credit institutions which carry out investment services and activities, data reporting services providers, market operators of trading venues, central securities depositories, credit rating agencies, securitisation repositories and administrators of benchmarks ("firms"), which use cloud services provided by third parties. This paper is also important for cloud service providers, because the draft guidelines set out therein seek to ensure that the risks that may arise for firms from the use of cloud services are properly addressed.

Table of Contents

1 Executive Summary

Reasons for publication

Firms are increasingly outsourcing to cloud service providers. Although cloud outsourcing can offer a number of benefits, including reduced costs and enhanced operational efficiency and flexibility, it raises challenges in terms of data protection and information security. Concentration risk can also arise, as a result of many firms using the same large cloud service providers, with potential negative outcomes for financial stability.

ESMA identified the need to develop guidance on outsourcing to cloud service providers following the European Commission's FinTech Action Plan[1] and feedback received from firms and stakeholders. Considering that the main risks associated with cloud outsourcing are similar across sectors, ESMA has considered the recent guidelines published by EBA and EIOPA, namely the EBA Guidelines on outsourcing arrangements[2], which have incorporated the EBA Recommendations on outsourcing to cloud service providers[3], and the EIOPA Guidelines on outsourcing to cloud service providers[4].

In accordance with Article 16(2) of Regulation (EU) No 1095/2010[5] (the 'ESMA Regulation'), as recently amended[6], this paper sets out for consultation draft ESMA guidelines on outsourcing to cloud service providers.

The purpose of these draft guidelines is to provide guidance on the outsourcing requirements applicable to firms where they outsource to cloud service providers. These draft guidelines are intended to help firms identify, address and monitor the risks that may arise from their cloud outsourcing arrangements (from making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities to providing for exit strategies).

Contents

Section 2 sets out the background of the guidelines. Section 3 sets out the proposed guidelines together with the questions for consultation. An overview of all the questions for

[1] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of Regions - FinTech Action plan: For a more competitive and innovative European financial sector, COM (2018) 109 final.
[2] EBA/GL/2019/02
[3] EBA/REC/2017/03
[4] EIOPA-BoS-20-002
[5] 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 (OJ L 331, 15.12.2010, p. 84).
[6] Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds (OJ L 334, 27.12.2019, p. 1).

consultation is provided in Appendix 1. The preliminary cost and benefit analysis is available in Appendix 2.

Next Steps

ESMA will consider the responses it receives to this consultation paper in Q3 2020 and expects to publish a final report and guidelines in Q 4 2020/Q1 2021.

2 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 certain benefits, including enhanced flexibility, operational efficiency, and cost effectiveness, with potential positive outcomes for firms and investors. Yet, cloud outsourcing comes with risks that need to be properly identified, monitored and mitigated, as outlined below. It is the firm's responsibility to identify and implement effective ways to manage risks in relation to the use of cloud services.

3. **Strategy, governance and oversight** – Cloud outsourcing may not be the outcome of a well thought out strategy and may not receive the necessary attention at firms' senior management level. Firms may consider the use of cloud services as an IT matter only, with little involvement and oversight from the management body. Perceiving the use of cloud services purely as an IT matter may lead to insufficient consideration of the business and regulatory requirements in the selection and design of the cloud solution. Also, firms may not have the necessary resources and processes in place to allow for an appropriate monitoring of the outsourced functions.

4. **Due diligence and risk assessment** – The lack of / or inadequate due diligence may restrict the ability of firms to make an informed decision when outsourcing to the cloud service provider. The decision to outsource may not involve a thorough assessment of the implied benefits and risks. In addition, ESMA has observed that cloud service providers often have a 'one-size-fit-all' approach and that firms tend to overlook the specificities of their data and business processes when defining their cloud outsourcing strategy. Such practices may lead to the adoption of cloud models that pose high risks, especially for critical business processes and non-public data. In addition, firms may not re-assess the risks arising from their cloud outsourcing arrangements as necessary, for example in case of changes in the circumstances of the cloud service provider.

5. **Accountability for the cloud and risk monitoring** – Firms may lose control over (part of) their IT framework, when outsourcing to cloud service providers. They may overly rely on cloud service providers, up to the point where they feel little accountability for the outsourced functions. They may not monitor as much as they should the systems where their data is kept and stored and be overconfident about the cloud implementation, also with the risk of unclear responsibilities and liabilities between firms and cloud service providers.

6. **Information security and disaster recovery risks** – Information security has been and will continue to be a key risk area for cloud services, considering the growing financial system interconnectedness and sophistication of cyber-attacks. Indeed, while cloud outsourcing has the potential to help firms mitigate certain information security risks, it can introduce or exacerbate others. Information security risks that may arise as a result of cloud outsourcing arrangements include the leak or loss of data, for example because of inadequate access control and identity management frameworks at the cloud service provider, hacking, legal uncertainty, and overreliance and/or inability to effectively use the information security frameworks of the cloud service provider. Inadequate monitoring controls may exacerbate these risks. The lack of or insufficient business continuity plans are another important source of risk, also considering that data location arrangements may not always provide for the effective recovery of data.

7. **Contractual limitations and lock-in risk** – Firms, especially smaller ones, often face challenges when negotiating with cloud service providers contractual terms and conditions that are suited to their specific needs and circumstances. There are also important data, application and infrastructure transfer risks, in case the cloud service provider no longer meets the expectations of the firm, changes or ceases its activities. The transfer to another provider or back in-house may be cumbersome and costly. Firms may not have well thought out plans and alternative solutions ('exit strategies') to exit their cloud outsourcing arrangement as and when necessary, and therefore be exposed to the risk of lock-in.

8. **Business continuity and other operational risks** – Firms may not be adequately prepared for events that generate important business continuity and operational risks. There may be failures or lack of appropriate controls regarding the effective interoperability and portability of data and exit strategies. The risk may be especially high where the firm has implementations both in the cloud and in local data centres, because of the elevated interoperability needs.

9. **Legal risks including governing law of contract and data location** – Outsourcing to the cloud entails legal risks, which firms may not always sufficiently consider. These risks relate to the governing law of the firms' contract with the cloud service provider, as well as the data location requirements. In particular, EU personal data location requirements[7] require close consideration.

10. **Impairing ESMA's and competent authorities' ability to perform their supervisory tasks** – Firms moving data to the cloud may present specific supervisory risks, e.g., in case supervisors do not have the necessary information to assess whether the firm manages its risks appropriately. Inadequate contractual arrangements may unduly restrict supervisors' right of access and audit, thus impairing ESMA's and competent authorities' ability to perform their supervisory tasks.

[7] 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 (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

11. 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 take into account the risk underlying the outsourcing of those functions.

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

13. 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.

3 Proposed guidelines

3.1 Scope

Who?

14. 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, (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 benchmarks, including, as of 1 January 2022, recognised third-country administrators of benchmarks which comply with the relevant requirements in the Benchmarks Regulation and administrators of critical benchmarks.

15. ESMA will also take these guidelines into account when assessing the extent to which (i) 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, and (ii) application of the relevant IOSCO principles by a third-country administrator of benchmarks seeking recognition is equivalent to compliance with the applicable requirements in the Benchmarks Regulation pursuant to Article 32(2) of the Benchmarks Regulation.

What?

16. 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)[8] 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;
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), 10 and 32 of the Benchmarks Regulation and Point 7 of Annex I of Commission Delegated Regulation (EU) 2018/1646.

When?

17. These guidelines apply from 30 June 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.

3.2 Legislative references, abbreviations and definitions

Legislative references

[8] 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.

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[9]
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[10]
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[11]
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 undertakings for collective investment in transferable securities (UCITS)[12]
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[13]
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[14]
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[15]
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[16]

[9] OJ L 331, 15.12.2010, p. 84
[10] OJ L 174, 1.7.2011, p. 1.
[11] OJ L 83, 22.3.2013, p. 1
[12] OJ L 302, 17.11.2009, p. 32
[13] OJ L 176, 10.7.2010, p. 42
[14] OJ L 78, 24.3.2016, p. 11
[15] OJ L 201, 27.7.2012, p. 1
[16] OJ L 337, 23.12.2015, p. 1

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[17]
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[18]
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 application for registration and extension of registration as a trade repository[19]
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[20]
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 ([21])
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[22]
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[23]
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

[17] OJ L 52, 23.2.2013, p. 41
[18] OJ L 52, 23.2.2013, p. 25
[19] OJ L 81, 22.3.2019, p. 45
[20] OJ L 173, 12.6.2014, p. 349
[21] OJ L 173, 12.6.2014, p. 84
[22] OJ L 87, 31.3.2017, p. 1
[23] OJ L 87, 31.3.2017, p. 350

	requirements and the publication of transactions for data reporting services providers[24]
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[25]
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[26]
CRA Regulation	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies[27]
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[28]
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[29]
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[30]
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

[24] OJ L 87, 31.3.2017, p. 126
[25] OJ L 257, 28.8.2014, p. 1.
[26] OJ L 65, 10.3.2017, p. 48
[27] OJ L 302, 17.11.2009, p. 1.
[28] OJ L 140, 30.5.2012, p. 32
[29] OJ L 347, 28.12.2017, p. 35.
[30] OJ L 171, 29.6.2016, p. 1

	provided in an application for authorisation and in an application for registration[31]

Abbreviations

CSP	Cloud service provider
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
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[32]	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;

[31] OJ L 274, 5.11.2018, p. 43
[32] Cloud computing is often abbreviated into 'cloud'. The term 'cloud' is used throughout the rest of the document for ease of reference.

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 on a CSP (for example through a sub-outsourcing chain) 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;
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[33], hybrid[34], private[35] and public[36] 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;

[33] 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;
[34] A cloud deployment model that uses at least two different cloud deployment models
[35] 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
[36] A cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider

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[37];
g) market operators of trading venues within the meaning of Article 4(1)(24) of MiFID II;
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 as defined in Article 3(1)(6) of the Benchmarks Regulation ("administrators of benchmarks"); recognised third-country administrators of benchmarks within the meaning of Article 32 of the Benchmarks Regulation which comply with the relevant requirements in the Benchmarks Regulation pursuant to Article 32(2) of that Regulation; administrators of critical benchmarks as defined in Article 3(1)(25) of the Benchmarks Regulation.

3.3 Purpose

18. 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 ESFS and to ensure the common, uniform and consistent application of the requirements referred to in Section 3.1 under the heading 'What?' where firms outsource to CSPs. In particular, they aim at helping firms and competent authorities identify, address and monitor the risks and challenges that arise from cloud outsourcing arrangements, from making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities to providing for exit strategies.

3.4 Compliance and reporting obligations

Status of the guidelines

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

[37] 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.

20. 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.

21. 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, by data reporting services providers, recognised third country administrators of benchmarks and administrators of critical benchmarks.

Reporting requirements

22. 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.

23. 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.

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

3.5 Guidelines on outsourcing to cloud services providers

Guideline 1. Governance, oversight and documentation

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

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

management body has the relevant technical skills[38]. Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and control of cloud outsourcing arrangements.

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

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

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

[38] 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).

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

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

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

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

Guideline 2. Pre-outsourcing analysis and due diligence

31. Before entering into any cloud outsourcing arrangement, a firm should:
    a) assess if the cloud outsourcing arrangement concerns a critical or important function;
    b) identify and assess all relevant risks of the cloud outsourcing arrangement;
    c) undertake appropriate due diligence on the prospective CSP;
    d) identify and assess any conflict of interest that the outsourcing may cause.

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

33. In case the cloud outsourcing arrangement concerns critical or important functions, a firm should also:
    a) assess all relevant risks that may arise as a result of the cloud outsourcing arrangement, including risks in relation to information and communication technology, information security, business continuity, legal and compliance, reputational risks, operational risks, and possible oversight limitations for the firm, arising from:
        i. the selected cloud service and the proposed deployment models;
        ii. the migration and/or the implementation processes;
        iii. the sensitivity of the function and the related data which are under consideration to be outsourced (or have been outsourced) and the security measures which would need to be taken;
        iv. the interoperability of the systems and applications of the firm and the CSP, namely their capacity to exchange information and mutually use the information that has been exchanged;
        v. the portability of the data of the firm, namely the capacity to easily transfer the firm's data from one CSP to another;

vi. the political stability, the security situation and the legal system (in particular the law, including insolvency law and enforcement as well as the requirements concerning the confidentiality of the firm's business related and/or personal data) of the countries (within or outside the EU) where the outsourced functions would be provided and where the outsourced data would be stored; in case of sub-outsourcing, the additional risks that may arise if the sub-outsourcer is located in a third country or a different country from the CSP and, in case of a sub-outsourcing chain, any additional risk which may arise, including in relation to the absence of a direct contact between the firm and the sub-outsourcer performing the outsourced function;

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

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

34. In case of outsourcing of critical or important functions, the due diligence should include an evaluation of the suitability of the CSP. When assessing the suitability of the CSP, a firm should ensure that the CSP has the business reputation, the skills, the resources (for example human, IT and financial), the organisational structure and, if applicable, the regulatory authorisation(s) or registration(s) to perform the critical or important function in a reliable and professional manner and to meet its obligations over the duration of the cloud outsourcing arrangement. Additional factors to be considered in the due diligence on the CSP include, but are not limited to:
    a) the management of information security and the protection of personal data;
    b) the service support, including support plans and contacts, and incident management processes;
    c) the business continuity and disaster recovery plans;

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

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

37. If the firm becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the CSP, the pre-outsourcing analysis and due diligence on the CSP should be promptly reviewed or re-performed.

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

Q3: Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

Guideline 3. Contractual requirements

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

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

41. In case of outsourcing of critical or important functions, the written agreement should set out at least:
    a) a clear description of the outsourced function;
    b) the start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the firm;
    c) the governing law of the agreement and, if any, the choice of jurisdiction;
    d) the parties' financial obligations;
    e) whether the sub-outsourcing of critical or important functions (or material parts thereof) is permitted, and, if so, the conditions to which the sub-outsourcing is subject, having regard to Guideline 7;
    f) the location(s) (namely countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s);
    g) provisions regarding information security and personal data protection, having regard to Guideline 4;
    h) the right for the firm to monitor the CSP's performance on a regular basis;
    i) the agreed service levels, which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;
    j) the reporting obligations of the CSP to the firm and, as appropriate, the obligations to submit reports relevant for the firm's security function and key functions, such as reports prepared by the internal audit function of the CSP;
    k) provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report incidents;
    l) whether the CSP should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;
    m) the requirements for the CSP to implement and test business continuity and disaster recovery plans;

n) the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access ('access rights') and to inspect ('audit rights') the books, premises, relevant systems and devices of the CSP to the extent necessary to monitor the CSP's performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6;
o) provisions to ensure that the data owned by the firm can be recovered by the firm as needed, having regard to Guideline 5.

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

Guideline 4. Information security

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

43. For that purpose, in case of outsourcing of critical or important functions, a firm, applying a risk-based approach, should at least:
a) *information security organisation:* ensure that there is a clear allocation of information security roles and responsibilities between the firm and the CSP, including in relation to threat detection, incident management and patch management, and ensure that the CSP is effectively able to fulfil its roles and responsibilities;
b) *access management*: ensure that strong authentication mechanisms (for example two factor authentication) are implemented and that access controls appropriately prevent unauthorised access to the firm's data and back-end cloud resources;
c) *encryption and key management:* consider the use of encryption technologies, where necessary, for data in transit, data in memory, data at rest and data back-ups, in combination with appropriate key management solutions to limit the risk of non-authorised access to the encryption keys (for example by preventing the CSP from storing and managing encryption keys or requiring separation of duties between key management and operations);
d) *operations and network security:* consider appropriate levels of segregating networks (for example tenant isolation in the shared environment of the cloud, operational separation as regards the web, application logic, operating system, network, Data Base Management System (DBMS) and storage layers) and processing environments (for example test, User Acceptance Testing, development, production)
e) *application programming interfaces (API):* consider mechanisms for the integration of the cloud services with the systems of the firm to ensure security of APIs (for example establishing and maintaining information security policies and procedures for APIs across multiple system interfaces, jurisdictions, and business functions to prevent unauthorised disclosure, modification or destruction of data);
f) *business continuity and disaster recovery*: ensure that effective business continuity and disaster recovery controls are in place (for example by setting minimum

capacity requirements, selecting hosting options that are geographically spread or requesting and reviewing documentation showing the transport route of the firm's data between the CSP's systems, as well as considering the possibility to replicate machine images to an independent storage location);

g) *data location*: adopt a risk-based approach to data storage and data processing location(s) (namely country or region);
h) *compliance & monitoring*: ensure that the CSP complies with internationally recognised information security standards and has implemented appropriate information security controls (for example by requesting the CSP to provide evidence that it conducts relevant information security reviews and by performing regular assessments and tests on the CSP's information security arrangements).

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

Guideline 5. Exit strategies

44. In case of outsourcing of critical or important functions, a firm should ensure that it is able to exit cloud outsourcing arrangements without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with the applicable legal requirements, as well as the confidentiality, integrity and availability of its data. To achieve this, a firm should:
    a) develop and implement exit plans that are comprehensive, documented and sufficiently tested. These plans should be updated as needed, including in case of changes in the outsourced function;
    b) identify alternative solutions and develop transition plans to remove the outsourced function and data from the CSP and, where applicable, any sub-outsourcer, and transfer them to the alternative CSP indicated by the firm or directly back to the firm. These solutions should be defined with regard to the challenges that may arise from the location of the data, taking the necessary measures to ensure business continuity during the migration phase;
    c) ensure that the cloud outsourcing written agreement includes an obligation for the CSP to orderly transfer the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy;
    d) ensure that any data removed or transferred is securely deleted from the systems of the CSP and, where applicable, of any sub-outsourcer (for example, by requesting a written confirmation by the CSP).

45. When developing the exit plans and solutions referred to in points (a) and (b) above ('exit strategy'), the firm should consider the following:
    a) define the objectives of the exit strategy;
    b) define the trigger events that could activate the exit strategy. These should include at least the termination of the cloud outsourcing arrangement at the initiative of the firm or the CSP and the failure or other serious discontinuation of the business activity of the CSP;

c) perform a business impact analysis that is commensurate to the function outsourced to identify what human and other resources would be required to implement the exit strategy;
d) assign roles and responsibilities to manage the exit strategy;
e) test the exit strategy, using a risk-based approach;
f) define success criteria of the transition.

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

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

Guideline 6. Access and audit rights

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

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

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

50. Without prejudice to their final responsibility regarding cloud outsourcing arrangements, in order to use audit resources more efficiently and decrease the organisational burden on the CSP and its clients, firms may use:
a) third-party certifications and external or internal audit reports made available by the CSP;
b) pooled audits performed jointly with other clients of the same CSP or pooled audits performed by a third-party auditor appointed by multiple clients of the same CSP.

51. In case of outsourcing of critical or important functions, a firm should make use of the third-party certifications and external or internal audit reports referred to in paragraph 50(a) only if it:
a) ensures that the scope of the certifications or the audit reports covers the CSP's systems (for example processes, applications, infrastructure, data centres), the key controls identified by the firm and the compliance with the relevant legal requirements;

b) thoroughly assesses the content of the certifications or audit reports on a regular basis and verify that the certifications or reports are not obsolete;
c) ensures that the CSP's key systems and controls are covered in future versions of the certification or audit report;
d) is satisfied with the certifying or auditing party (for example with regard to its qualifications, expertise, re-performance/verification of the evidence in the underlying audit file as well as rotation of the certifying or auditing company);
e) is satisfied that the certifications are issued and that the audits are performed according to appropriate standards and include a test of the effectiveness of the key controls in place;
f) has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP;
g) retains the contractual right to perform individual on-site audits at its discretion with regard to the outsourced function.

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

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

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

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

Guideline 7. Sub-outsourcing

55. If sub-outsourcing of critical or important functions (or a part thereof) is permitted, the cloud outsourcing written agreement between the firm and the CSP should:
a) specify any part or aspect of the outsourced function that are excluded from potential sub-outsourcing;
b) indicate the conditions to be complied with in case of sub-outsourcing;
c) specify that the CSP is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the CSP and the firm are continuously met;
d) include an obligation for the CSP to notify the firm of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the

CSP to meet its obligations under the cloud outsourcing arrangement with the firm. The notification period to be set should allow the firm sufficient time to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them, as indicated in point (e) below;

e) ensure that the firm has the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect;
f) ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing, i.e. where the CSP proceeds with the sub-outsourcing without notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement.

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

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

Guideline 8. Written notification to competent authorities

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

58. The firm's written notification should include, taking into account the principle of proportionality, at least the following information:
    a) a description of the outsourced function;
    b) the start date of the cloud outsourcing agreement and, as applicable, the next contract renewal date, the end date and/or notice periods for the CSP and for the firm;
    c) the name and the brand name (if any) of the CSP, the country of registration, the corporate registration number, the legal entity identifier (where available), the registered address, the relevant contact details, and the name of the parent company (if any);
    d) the governing law of the cloud outsourcing agreement and, if any, the choice of jurisdiction;
    e) the cloud deployment models and the specific nature of the data to be held by the CSP and the locations (namely countries) where such data may be stored and processed;
    f) where applicable, the names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the country or region where the sub-outsourcers are registered, where the sub-outsourced service will be performed, where the data will be stored and where the data may be processed;
    g) a summary of the reasons why the outsourced function is considered critical or important;
    h) the date of the most recent assessment of the criticality or importance of the outsourced function;

i) the date of the most recent risk assessment/audit together with a brief summary of the main results, and the date of the next planned risk assessment/audit;
j) the individual or decision-making body in the firm that approved the cloud outsourcing arrangement.

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

Guideline 9. Supervision of cloud outsourcing arrangements

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

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

61. Competent authorities should assess on a risk-based approach whether firms:
    a) have in place the relevant governance, resources and operational processes to appropriately and effectively enter into, implement, and oversee cloud outsourcing arrangements;
    b) identify and manage all relevant risks related to cloud outsourcing.

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

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

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

Q12: What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organisation, where relevant.

Appendix 1 - Summary of questions

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

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

Q3: Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

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

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

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

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

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

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

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

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

Q12: What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organisation, where relevant.

Appendix 2 - Preliminary cost-benefit analysis

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 draft ESMA guidelines

We set out below a preliminary assessment of the expected benefits and costs of the proposed guidelines for consultation.

Benefits

ESMA believes that the introduction of the proposed guidelines will:

a) support firms in their prudent transition to the cloud, by providing clarity on the applicable regulatory requirements, 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

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.

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;
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 pre-selection, due diligence and oversight of the cloud service providers;

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

Conclusions

In light of the above, ESMA believes that the overall (compliance) costs associated with the implementation of the guidelines will be fully compensated by the benefits arising from the

enhanced regulatory certainty and risk management framework. All Firms will benefit from the guidelines.

ESMA also considers that the proposed guidelines support greater harmonisation in the interpretation and consistent application of the provisions listed in Section 3.1 under the heading ‘What?’ 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.

Finally, ESMA believes that the adoption of the guidelines is the best tool to provide clear guidance to firms on how to enter into 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).