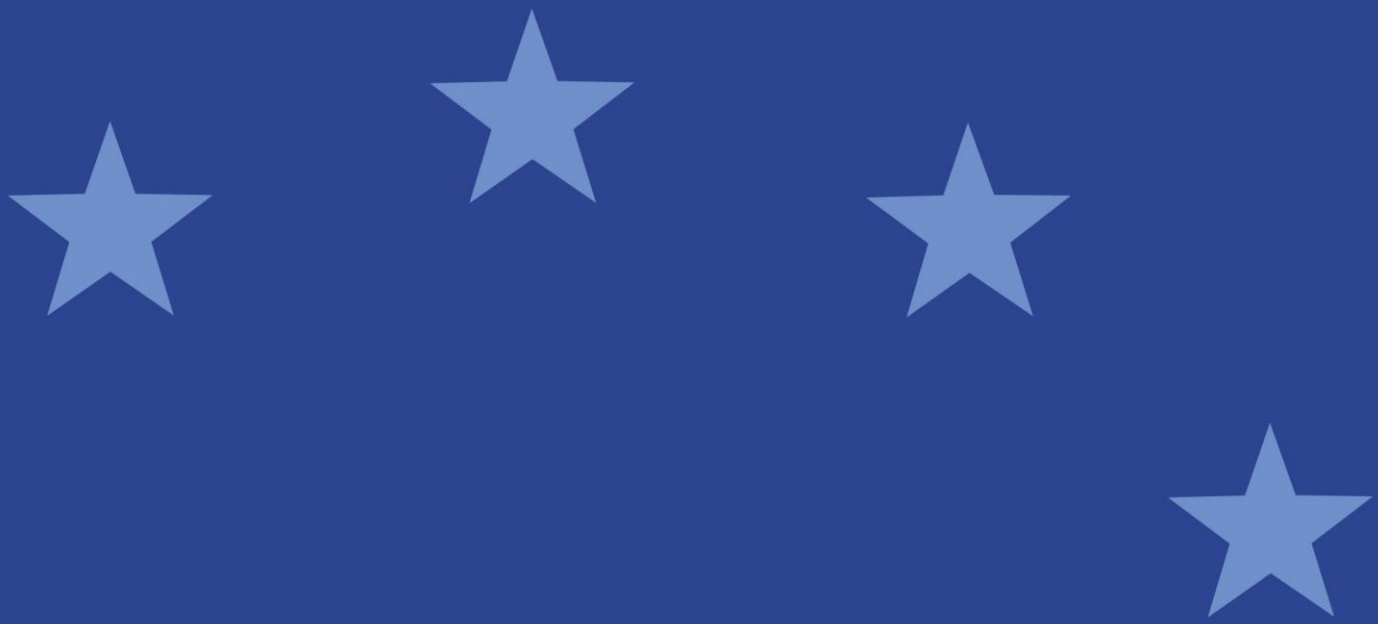
esma European Securities and Markets Authority

Guidelines

On outsourcing to cloud service providers



10/05/2021| ESMA50-164-4285

Table of Contents

I. 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)1 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;

[1] 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.

II. 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[2]
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[3]
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[4]
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

[2] OJ L 331, 15.12.2010, p. 84
[3] OJ L 174, 1.7.2011, p. 1.
[4] OJ L 83, 22.3.2013, p. 1

	undertakings for collective investment in transferable securities (UCITS)[5]
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[6]
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[7]
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[8]
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[9]
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[10]
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[11]
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

[5] OJ L 302, 17.11.2009, p. 32
[6] OJ L 176, 10.7.2010, p. 42
[7] OJ L 78, 24.3.2016, p. 11
[8] OJ L 201, 27.7.2012, p. 1
[9] OJ L 337, 23.12.2015, p. 1
[10] OJ L 52, 23.2.2013, p. 41
[11] OJ L 52, 23.2.2013, p. 25

	application for registration and extension of registration as a trade repository[12]
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[13]
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 ([14])
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[15]
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[16]
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[17]
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[18]
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[19]

[12] OJ L 81, 22.3.2019, p. 45
[13] OJ L 173, 12.6.2014, p. 349
[14] OJ L 173, 12.6.2014, p. 84
[15] OJ L 87, 31.3.2017, p. 1
[16] OJ L 87, 31.3.2017, p. 350
[17] OJ L 87, 31.3.2017, p. 126
[18] OJ L 257, 28.8.2014, p. 1.
[19] 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[20]
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[21]
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[22]
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[23]
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[24]
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[25]

Abbreviations

CSP	Cloud service provider
ESMA	European Securities and Markets Authority

[20] OJ L 302, 17.11.2009, p. 1.
[21] OJ L 140, 30.5.2012, p. 32
[22] OJ L 347, 28.12.2017, p. 35.
[23] OJ L 171, 29.6.2016, p. 1
[24] OJ L 274, 5.11.2018, p. 43
[25] 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[26]	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;

[26] 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[27], hybrid[28], private[29] and public[30] 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[31]; g) market operators of trading venues within the meaning of Article 4(1)(24) of MiFID II;

[27] 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;
[28] A cloud deployment model that uses at least two different cloud deployment models
[29] 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
[30] A cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider
[31] 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.

III. 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.

IV. 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.

V. 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[32]. 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.

[32] 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.