EBA/REC/2017/03

20 December 2017

Final Report

Recommendations on outsourcing to cloud service providers

Contents

1. Executive summary

These recommendations are intended to provide guidance on outsourcing by institutions to cloud service providers.

Although general outsourcing guidelines have been in place since 2006 in the form of the Committee of European Banking Supervisors guidelines on outsourcing (CEBS guidelines),[1] the outsourcing framework is constantly evolving. In recent years, there has been increasing interest on the part of institutions in using the services of cloud service providers. Although the CEBS guidelines remain applicable to general outsourcing by institutions, these recommendations provide additional guidance for the specific context of institutions that outsource to cloud service providers.

These recommendations apply to credit institutions and investment firms as defined in Article 4(1) of Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR). The principle of proportionality applies throughout the recommendations, which should be employed in a manner proportionate to the size, structure and operational environment of the institution, as well as the nature, scale and complexity of its activities.

The guidance set out in these recommendations starts with specific directions on how to assess the materiality of cloud outsourcing. In line with the CEBS guidelines, the materiality of cloud outsourcing determines whether an institution is required to adequately inform its competent authority about it. Specific guidance is included on the process that institutions should follow in informing their competent authorities about material cloud outsourcing and the information to be provided.

In view of the importance of contractually securing both the right to audit for institutions and competent authorities and the right of physical access to the business premises of cloud service providers, supervisory expectations for outsourcing institutions in these respects are further explained.

To take account of the specificities of cloud outsourcing, the recommendations include guidance on the security of the data and systems used. They also address the treatment of data and data processing locations in the context of cloud outsourcing. Institutions should adopt a risk-based approach in this respect and implement adequate controls and measures, such as the use of encryption technologies for data in transit, data in memory and data at rest.

The recommendations include specific requirements for institutions to mitigate the risks associated with 'chain' outsourcing, where the cloud service provider subcontracts elements of the service to other providers. The use of subcontractors by the cloud service provider should not affect the services provided under the outsourcing agreement, and appropriate arrangements should be in place for the orderly transfer of the activity, data or services from the subcontractor to another service provider if necessary.

[1] CEBS guidelines on outsourcing, 14 December 2006, available online at http://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

Contingency plans and exit strategies form an important part of any cloud outsourcing arrangement. The recommendations provide guidance for institutions on the contractual and organisational arrangements for contingency plans and exit strategies that should be in place in the context of cloud outsourcing.

The EBA has held a public consultation on these recommendations, and the text has been amended to reflect the outcomes of the consultation. A detailed analysis of the feedback received and the EBA's responses is provided in this final report.

Next steps

The recommendations will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report whether they comply with the recommendations will be two months after the publication of the translations. The recommendations will apply from 1 July 2018.

2. Background and rationale

1. Under Article 16 of Regulation (EU) No 1093/2010[2] (the EBA Regulation), the EBA is required to issue guidelines and recommendations addressed to competent authorities and financial institutions, with a view to establishing consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of European Union law.

2. The purpose of these EBA recommendations is to specify the supervisory requirements and processes that apply when institutions outsource to cloud service providers. To that end, these recommendations build on the guidance provided by the CEBS guidelines.

3. The EBA identified the need to develop specific guidance on outsourcing to cloud service providers following interactions with several stakeholders. It appears that there is a high level of uncertainty regarding the supervisory expectations that apply to outsourcing to cloud service providers and that this uncertainty forms a barrier to institutions using cloud services. There are some differences in the national regulatory and supervisory frameworks for cloud outsourcing, for example with regard to the information requirements that institutions need to comply with.

4. Compared with more traditional forms of outsourcing offering tailor-made solutions to clients, cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale. Although cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual institutions but also at industry level, as large suppliers of cloud services can become a single point of failure when many institutions rely on them.

5. The aims of these recommendations are to:

(a) provide the necessary clarity for institutions should they wish to adopt and reap the benefits of cloud computing while ensuring that risks are appropriately identified and managed;
(b) foster supervisory convergence regarding the expectations and processes applicable in relation to the cloud.

6. The recommendations focus on the most important areas for further supervisory alignment and/or clarification identified by stakeholders.

7. An area in which different practices were observed among Member States was the duty for an outsourcing institution to adequately inform its competent authority about material (cloud) outsourcing. Therefore, specific guidance is included on the process that institutions should

[2] Regulation of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.12.2010, p. 12.

follow in informing their competent authorities about material cloud outsourcing and the information to be provided.

8. The right to audit is a key right laid down in the principles of the CEBS guidelines that is restated in these recommendations. Further guidance is provided on how institutions can exercise this right to audit in a risk-based and proportionate manner, taking account of concerns with regard to organisational burdens for both the outsourcing institution and the service provider, as well as of practical, security and confidentiality concerns regarding physical access to certain types of business premises and access to data in multi-tenant cloud environments (where several cloud service users share access to a set of physical and virtual resources, although their data are kept separate from one another).

9. The CEBS guidelines already provide guidance on issues such as information confidentiality and system availability. These recommendations elaborate on the need for integrity and traceability, establishing an approach to assessing security when institutions outsource activities to cloud service providers. The recommendations aim to address heterogeneity in supervisory expectations regarding the technical security of cloud computing services.

10. The performance and quality of the cloud service provider's service delivery and the level of operational risk that it may cause to the outsourcing institution are largely determined by the ability of the cloud service provider to appropriately protect the confidentiality, integrity and availability of data (in transit or at rest) and of the systems and processes that are used to process, transfer or store these data. Appropriate traceability mechanisms aimed at keeping records of technical and business operations are also key to detecting malicious attempts to breach the security of data and systems. In accordance with the principle of proportionality, security expectations should take into account the need to protect the data and systems under consideration.

11. As cloud service providers often operate a geographically dispersed computing infrastructure that entails the regional and/or global distribution of data storage and processing, the recommendations set out specific requirements for data and data processing locations in the context of cloud outsourcing. Notwithstanding this guidance, Union and national laws apply in this respect, and, in particular with respect to any obligations or contractual rights referred to in these recommendations, attention should be paid to data protection rules and professional secrecy requirements.

12. Chain outsourcing (subcontracting) is extensively used; in this regard, cloud outsourcing is more dynamic in nature than traditional outsourcing set-ups. Therefore, there is a need for greater certainty about the conditions under which subcontracting can take place in the case of cloud outsourcing. In this context, the recommendations specify that subcontracting requires *ex ante* notification to the outsourcing institution, whose consent, however, is not required, as this would be overly burdensome from a practical perspective. The institution should, in any case, always retain the right to terminate the contract if planned changes to subcontracted services would have an adverse effect on the risk assessment of the outsourced services.

13. The recommendations are not exhaustive, and they should be read in conjunction with the CEBS guidelines.

14. As regards the scope of these recommendations, a similar approach to that of the CEBS guidelines was taken. In relation to institutions offering investment services, an analysis was performed to ensure that these recommendations are fully consistent with the relevant provisions of MiFID II on outsourcing[3] and the related implementing regulation.[4]

15. The clarifications provided in these recommendations will eventually feed into the updating of the CEBS guidelines by the EBA.

[3] 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, available online at https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en; see in particular Article 16.

[4] 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, available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0565&from=DE; see in particular Articles 30-32.

EBA/REC/2017/03

20/12/2017

3. Recommendations

on outsourcing to cloud service providers

1. Compliance and reporting obligations

Status of these recommendations

1. This document contains recommendations issued pursuant to Article 16 of Regulation (EU) No 1093/2010.[5] In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with these recommendations.

2. Recommendations set out the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to which recommendations apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where recommendations are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these recommendations, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/REC/2017/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[5] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter and scope of application

1. These recommendations further specify conditions for outsourcing as referred to in the CEBS guidelines on outsourcing of 14 December 2006 and apply to outsourcing by institutions as defined in point (3) of Article 4(1) of Regulation (EU) No 575/2013 to cloud service providers.

Addressees

2. These recommendations are addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010 and to institutions as defined in point (3) of Article 4(1) of Regulation No 575/2013.[6]

Definitions

3. Unless otherwise specified, terms used and defined in Directive 2013/36/EU [7] on capital requirements and in the CEBS guidelines have the same meaning in the recommendations. In addition, for the purposes of these recommendations the following definitions apply:

Cloud services	Services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Public cloud	Cloud infrastructure available for open use by the general public.
Private cloud	Cloud infrastructure available for the exclusive use by a single institution.
Community cloud	Cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group.
Hybrid cloud	Cloud infrastructure that is composed of two or more distinct cloud infrastructures.

[6] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

[7] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

3. Implementation

Date of application

5. These recommendations apply from 1 July 2018.

4. Recommendations on outsourcing to cloud service providers

4.1 Materiality assessment

1. Outsourcing institutions should, prior to any outsourcing of their activities, assess which activities should be considered as material. Institutions should perform this assessment of activities' materiality on the basis of guideline 1(f) of the CEBS guidelines and, as regards outsourcing to cloud service providers in particular, taking into account all of the following:

    (a) the criticality and inherent risk profile of the activities to be outsourced, i.e. are they activities that are critical to the business continuity/viability of the institution and its obligations to customers;

    (b) the direct operational impact of outages, and related legal and reputational risks;

    (c) the impact that any disruption of the activity might have on the institution's revenue prospects;

    (d) the potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers.

4.2 Duty to adequately inform supervisors

2. Outsourcing institutions should adequately inform the competent authorities of material activities to be outsourced to cloud service providers. Institutions should perform this on the basis of paragraph 4.3 of the CEBS guidelines and, in any case, make available to the competent authorities the following information:

    (a) the name of the cloud service provider and the name of its parent company (if any);
    (b) a description of the activities and data to be outsourced;
    (c) the country or countries where the service is to be performed (including the location of data);
    (d) the service commencement date;
    (e) the last contract renewal date (where applicable);
    (f) the applicable law governing the contract;
    (g) the service expiry date or next contract renewal date (where applicable).

3. Further to the information provided in accordance with the previous paragraph, the competent authority may ask the outsourcing institution for additional information on its risk analysis for the material activities to be outsourced, such as:

(a) whether the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;
(b) whether the outsourcing institution has an exit strategy in case of termination by either party or disruption of provision of the services by the cloud service provider;
(c) whether the outsourcing institution maintains the skills and resources necessary to adequately monitor the outsourced activities.

4. The outsourcing institution should maintain an updated register of information on all its material and non-material activities outsourced to cloud service providers at institution and group level. The outsourcing institution should make available to the competent authority, on request, a copy of the outsourcing agreement and related information recorded in that register, irrespective of whether or not the activity outsourced to a cloud service provider has been assessed by the institution as material.

5. In the register referred to in the previous paragraph, at least the following information should be included:

(a) the information referred to in paragraph 2(a) to (g), if not yet provided;
(b) the type of outsourcing (the cloud service model and the cloud deployment model, i.e. public/private/hybrid/community cloud);
(c) the parties receiving cloud services under the outsourcing agreement;
(d) evidence of the approval for outsourcing by the management body or its delegated committees, if applicable;
(e) the names of any subcontractors if applicable;
(f) the country where the cloud service provider/main subcontractor is registered;
(g) whether the outsourcing has been assessed as material (yes/no);
(h) the date of the institution's last materiality assessment of the outsourced activities;
(i) whether the cloud service provider/subcontractor(s) supports business operations that are time critical (yes/no);
(j) an assessment of the cloud service provider's substitutability (as easy, difficult or impossible);
(k) identification of an alternate service provider, where possible;
(l) the date of the last risk assessment of the outsourcing or subcontracting arrangement.

4.3 Access and audit rights

For institutions

6. On the basis of guideline 8(2)(g) of the CEBS guidelines and for the purposes of cloud outsourcing, outsourcing institutions should further ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligation:

(a) to provide to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor full access to its business premises

(head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services outsourced (right of access);

(b) to confer to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor, unrestricted rights of inspection and auditing related to the outsourced services (right of audit).

7. The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. If the performance of audits or the use of certain audit techniques might create a risk for another client's environment, alternative ways to provide a similar level of assurance required by the institution should be agreed on.

8. The outsourcing institution should exercise its rights to audit and access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources, it should consider using at least one of the following tools:

(a) Pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by a third party appointed by them, in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the cloud service provider.

(b) Third-party certifications and third-party or internal audit reports made available by the cloud service provider, provided that:

i. The outsourcing institution ensures that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and the controls identified as key by the outsourcing institution.
ii. The outsourcing institution thoroughly assesses the content of the certifications or audit reports on an ongoing basis, and in particular ensures that key controls are still covered in future versions of an audit report and verifies that the certification or audit report is not obsolete.
iii. The outsourcing institution is satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file).
iv. The certifications are issued and the audits are performed against widely recognised standards and include a test of the operational effectiveness of the key controls in place.
v. The outsourcing institution has the contractual right to request the expansion of scope of the certifications or audit reports to some systems and/or controls that are relevant. The number and frequency of such requests for scope modification should be reasonable, and legitimate from a risk management perspective.

9. Considering that cloud solutions have a high level of technical complexity, the outsourcing institution should verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the cloud service provider's appointed auditors – or, as

appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the right skills and knowledge to perform effective and relevant audits and/or assessments of cloud solutions.

For competent authorities

10. On the basis of guideline 8(2)(h) of the CEBS guidelines and for the purposes of cloud outsourcing, outsourcing institutions should ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligation:

    (a) to provide to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) full access to the cloud service provider's business premises (head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services to the outsourcing institution (right of access);

    (b) to confer to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) unrestricted rights of inspection and auditing related to the outsourced services (right of audit).

11. The outsourcing institution should ensure that the contractual arrangements do not impede its competent authority to carry out its supervisory function and objectives.

12. Information that competent authorities obtain from the exercise of the rights of access and audit should be subject to the professional secrecy and confidentiality requirements referred to in Article 53 et seq. of Directive 2013/36/EU (CRD IV). Competent authorities should refrain from entering into any kind of contractual agreement or declaration that would prevent them from abiding by the provisions of Union law on confidentiality, professional secrecy and information exchange.

13. Based on the findings of its audit, the competent authority should address any deficiencies identified, if necessary, by imposing measures directly on the outsourcing institution.

4.4 In particular for the right of access

14. The agreement referred to in paragraphs 6 and 10 should include the following provisions:

    (a) The party intending to exercise its right of access (institution, competent authority, auditor or third party acting for the institution or the competent authority) should before a planned onsite visit provide notice in a reasonable time period of the onsite visit to a relevant business premise, unless an early prior notification has not been possible due to an emergency or crisis situation.

(b) The cloud service provider is required to fully cooperate with the appropriate competent authorities, as well as the institution and its auditor, in connection with the onsite visit.

4.5 Security of data and systems

15. As stated by guideline 8(2)(e) of the CEBS guidelines, the outsourcing contract should oblige the outsourcing service provider to protect the confidentiality of the information transmitted by the financial institution. In line with guideline 6(6)(e) of the CEBS guidelines, institutions should implement arrangements to ensure the continuity of services provided by outsourcing service providers. Building on guidelines 8(2)(b) and 9 of the CEBS guidelines, the respective needs of outsourcing institutions with respect to quality and performance should feed into written outsourcing contracts and service level agreements. These security aspects should also be monitored on an ongoing basis (guideline 7).

16. For the purposes of the previous paragraph, the institution should perform, prior to outsourcing and for the purpose of informing the relevant decision, at least the following:

(a) identify and classify its activities, processes and related data and systems as to the sensitivity and required protections;

(b) conduct a thorough risk-based selection of the activities, processes and related data and systems which are under consideration to be outsourced to a cloud computing solution;

(c) define and decide on an appropriate level of protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing. Institutions should also consider specific measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture.

17. Subsequently, institutions should ensure that they have in place an agreement in writing with the cloud service provider in which, among other things, the latter's obligations under paragraph 16(c) are set out.

18. Institutions should monitor the performance of activities and security measures in line with guideline 7 of the CEBS guidelines, including incidents, on an ongoing basis and review as appropriate whether their outsourcing of activities complies with the previous paragraphs; they should promptly take any corrective measures required.

4.6 Location of data and data processing

19. As stated in guideline 4(4) of the CEBS guidelines, institutions should take special care when entering into and managing outsourcing agreements undertaken outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authority.

20. The outsourcing institution should adopt a risk-based approach to data and data processing location considerations when outsourcing to a cloud environment. The assessment should address the potential risk impacts, including legal risks and compliance issues, and oversight limitations related to the countries where the outsourced services are or are likely to be provided and where the data are or are likely to be stored. The assessment should include considerations on the wider political and security stability of the jurisdictions in question; the laws in force in those jurisdictions (including laws on data protection); and the law enforcement provisions in place in those jurisdictions, including the insolvency law provisions that would apply in the event of a cloud service provider's failure. The outsourcing institution should ensure that these risks are kept within acceptable limits commensurate with the materiality of the outsourced activity.

4.7 Chain outsourcing

21. As stated in guideline 10 of the CEBS guidelines, institutions should take account of the risks associated with 'chain' outsourcing, where the outsourcing service provider subcontracts elements of the service to other providers. The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider. Furthermore, the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement.

22. The outsourcing agreement between the outsourcing institution and the cloud service provider should specify any types of activities that are excluded from potential subcontracting and indicate that the cloud service provider retains full responsibility for and oversight of those services that it has subcontracted.

23. The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution of any planned significant changes to the subcontractors or the subcontracted services named in the initial agreement that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period for those changes should be contractually pre-agreed to allow the outsourcing institution to carry out a risk assessment of the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.

24. In case a cloud service provider plans changes to a subcontractor or subcontracted services that would have an adverse effect on the risk assessment of the agreed services, the outsourcing institution should have the right to terminate the contract.

25. The outsourcing institution should review and monitor the performance of the overall service on an ongoing basis, regardless of whether it is provided by the cloud service provider or its subcontractors.

4.8 Contingency plans and exit strategies

26. As stated in guidelines 6.1, 6(6)(e) and 8(2)(d) of the CEBS guidelines, the outsourcing institution should plan and implement arrangements to maintain the continuity of its business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree. These arrangements should include contingency planning and a clearly defined exit strategy. Furthermore, the outsourcing contract should include a termination and exit management clause that allows the activities being provided by the outsourcing service provider to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution.

27. An outsourcing institution should also ensure that it is able to exit cloud outsourcing arrangements, if necessary, without undue disruption to its provision of services or adverse effects on its compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients. To achieve this, an outsourcing institution should:

    (a) develop and implement exit plans that are comprehensive, documented and sufficiently tested where appropriate;

    (b) identify alternative solutions and develop transition plans to enable it to remove and transfer existing activities and data from the cloud service provider to these solutions in a controlled and sufficiently tested manner, taking into account data location issues and maintenance of business continuity during the transition phase;

    (c) ensure that the outsourcing agreement includes an obligation on the cloud service provider to sufficiently support the outsourcing institution in the orderly transfer of the activity to another service provider or to the direct management of the outsourcing institution in the event of the termination of the outsourcing agreement.

28. When developing exit strategies, an outsourcing institution should consider the following:

    (a) develop key risk indicators to identify an unacceptable level of service;

    (b) perform a business impact analysis commensurate with the activities outsourced to identify what human and material resources would be required to implement the exit plan and how much time it would take;

(c) assign roles and responsibilities to manage exit plans and transition activities.

(d) define success criteria of the transition.

29. The outsourcing institution should include indicators that can trigger the exit plan in its ongoing service monitoring and oversight of the services provided by the cloud service provider.

5. Accompanying documents

5.1 Draft cost-benefit analysis/impact assessment

These recommendations are designed to complement the CEBS guidelines, which provide guidance on the process of outsourcing activities to cloud service providers for institutions using such services.

According to Article 16(2) of the EBA Regulation (Regulation (EU) No 1093/2010 of the European Parliament and of the Council), any recommendations developed by the EBA shall be accompanied by an analysis looking at 'the potential related costs and benefits'. This analysis should provide the reader with an overview of the findings as regards the baseline scenario, problem identification, the options identified to remove the problem and their potential impacts.

This section presents an impact assessment with a cost-benefit analysis of the provisions included in the recommendations described in this consultation paper. Given the nature of the study, the analysis is high level and qualitative in nature.

A. Problem identification

The core problems that the current recommendations aim to address are the outdated framework on the process of outsourcing to cloud service providers and the lack of harmonised regulatory practices across jurisdictions.

Since the introduction of the CEBS guidelines in December 2006, both the volume of financial information/data to be managed by institutions and demand for outsourcing to cloud service providers have been increasing. Currently, the regulatory framework does not provide certainty in relation to the outsourcing process and this uncertainty may lead to market inefficiency; for example, although there is demand for outsourcing, institutions may decide not to opt for this option on account of regulatory uncertainty. Furthermore, the lack of an effective regulatory framework is expected to entail a higher degree of operational risk in relation to outsourcing. Data and systems security, confidentiality, legal and reputational risk and the exchange of information among the parties (outsourcing institutions, cloud service providers, subcontractors and the competent authorities) are crucial aspects of the process that the current regulatory framework does not fully cover in the context of cloud outsourcing. The absence of a more effective framework increases the risk profile of such events: the lack of specific guidance and of a more detailed assessment to be carried out by supervisors to assess outsourcing risk may lead to incomplete risk assessments of institutions in the prudential supervisory framework.

Furthermore, the implementation of the CEBS guidelines varies across jurisdictions. The core gap that the current draft recommendations aim to address is the lack of guidance on the

regulatory framework and on the supervisory assessment of outsourcing risks in EU institutions, and the resulting room for inconsistency in assessing outsourcing risk across jurisdictions. This leads to a lack of comparability of supervisory practices across the EU, and such comparability is crucial given the cross-border nature of cloud services. Inconsistency in the treatment of potential risks related to cloud services may also lead to an uneven playing field across jurisdictions and institutions.

B. Baseline scenario

The CEBS guidelines (2006) are the current guiding framework that regulates outsourcing activities, and most Member States have comprehensively transposed the CEBS guidelines: a survey carried out by the EBA (completed on 18 September 2015) indicated that of the 24 national frameworks [8] 53% totally transposed, 38% partially transposed and 8% did not transpose the CEBS guidelines. Overall, 88% of jurisdictions had incorporated the CEBS concept of 'material activities', i.e. critical, into their frameworks, although in a majority of cases (54%) they had not adhered strictly to the four CEBS criteria. In all jurisdictions, the general framework on outsourcing applies to cloud computing.

In terms of specific national frameworks on cloud computing, the survey revealed that cloud computing is not subject to a specific framework in 13 Member States and 1 EEA country[9] (or 58% of jurisdictions).[10] In 12 Member States (or 50% of jurisdictions)[11] a specific framework applies. The following activities, either specified in the CEBS guidelines or under a specific national framework, are the (most common) current practices:

Formalities required

- notification requirement (*ex ante* information);
- authorisation or *nihil obstat* from the supervisor;
- subject to security check by the supervisor;
- *ex post* information (e.g. annual report).

Mandatory contractual clauses

- termination of service and exit clause;
- direct audit rights for the supervisors in relation to the provider;
- full audit rights for the regulated institution;
- agreement of the regulated institution on the location of the data/services;

[8] A total of 25 competent authorities from 24 Member States participated in the survey.

[9] Please note that the data are based on the responses to the survey and on bilateral interactions during the production of the consultation paper.

[10] These are AT, BG, CY, DE, DK, EE, EL, FI, HR, IE, LT, NO, PT and SK.

[11] These are BE, CZ, ES, FR, HU, IT, LU, LV, NL, PL, SE and UK.

- capacity of the regulated institution to re-enter the data/services;
- agreement of the regulated institution on the law governing the contract and the data/services;
- approval of the regulated institution prior to any move of the data/services.

As a result, the technical requirements set out by Member States are in most cases not very detailed and approximately 50% of Member States have principle-based regulatory frameworks on this matter. The mapping of the current practices shows that regulatory and supervisory frameworks appears multiple and potentially difficult to well understand for institutions with a cross-border presence, or even for their cloud service providers. Although they are similar on some points, each national framework has its own nuances, which does not facilitate an interpretation of the current supervisory expectations in the EU. Without regulatory intervention, the current situation with the abovementioned shortcomings is expected to continue.

C. Policy objectives

The main objective of the draft recommendations is to specify a set of principle-based rules that complement and update the CEBS guidelines and that competent authorities can apply within their regulatory and supervisory frameworks on the cloud outsourcing process and the associated risks. Specifically, the recommendations aim to provide the competent authorities with an overall regulatory framework, tools for their risk assessments and clarity with regard to the process. This is further expected to lead to the harmonisation of practices and a level playing field across jurisdictions. In this way, the current draft recommendations are expected to respond proactively to challenges relating to the prudential supervision of specific ICT-related risks.

The table below summarises the objectives of the current draft recommendations:

Operational objectives	Specific objectives	General objectives
Updating and complementing the current framework on cloud outsourcing (CEBS guidelines) to respond to the challenges arising from the current regulatory/supervisory framework.	Establishing common practices across jurisdictions to increase the risk assessment capabilities with respect to cloud services in the banking sector and to reduce uncertainty while providing enough room for flexibility to accommodate new challenges.	Ensuring the consistent application of regulatory/supervisory criteria and strengthening prudential supervision.

D. Assessment of the technical options

Introduction of the recommendations versus the status quo

The EBA believes that, without the introduction of the additional guidance, the CEBS guidelines fail to provide an adequate regulatory framework for institutions and competent authorities in their handling of cloud outsourcing activities in the banking sector. Under the status quo, the current problems are expected to continue.

The option of introducing these recommendations was taken to provide additional guidance to complement the general CEBS outsourcing guidelines where needed. This is, as previously discussed, either because a need for further convergence of supervisory practices/expectations was identified or because the areas in question were particularly relevant in the specific context of cloud outsourcing. The recommendations avoid repeating what is already in the general CEBS outsourcing guidelines, which remain valid also in the context of cloud outsourcing.

With regard to the cost of compliance with the recommendations, it is reasonable to expect that, in jurisdictions where the current practices overlap with or are similar to what is proposed in the recommendations, institutions and competent authorities will incur less additional administrative cost. In other words, the more similar the current practices are to the recommendations, the less costly the transition will be. Section B on the baseline scenario above provides some Member State-level analysis of this aspect.

If a national framework does not comply with the current CEBS guidelines, i.e. the CEBS guidelines have not been transposed,[12] the institutions in the Member State in question will need to spend more additional time and resources on:

- producing the analyses and information required under these recommendations, for example in relation to the criteria for the materiality assessment (section 4.1) and the disclosure to supervisors (section 4.2);
- reviewing legal issues on access and audit rights (section 4.3) and particular aspects of right of access (section 4.4);
- improving the infrastructure to ensure appropriate risk assessments and an appropriate level of protection of data confidentiality, continuity of activities outsourced, and the security, integrity and traceability of data systems (sections 4.5, 4.6 and 4.7); and
- developing contingency plans and exit strategies (section 4.8).

Similarly, competent authorities would need to spend more additional time and resources on processing the information received from the institutions.

[12] Note that this is an assumption and that in practice the baseline scenario analysis shows that most Member States are either fully or partially in compliance with the CEBS guidelines. Even where the CEBS guidelines have not been transposed, the Member States in question implement their provisions in their supervisory practices.

However, since most institutions currently have similar procedures in place, the marginal cost of implementing these supervisory changes is expected to be small or negligible.

Exhaustive and prescribed list of requirements versus non-exhaustive list

Firstly, instead of providing specific guidance for specific types of cloud outsourcing (e.g. SaaS, IaaS and PaaS), the EBA prefers, as far as possible, to introduce technology-neutral and future-proof recommendations. This should allow a more proactive and flexible framework that can respond more swiftly to the changing context of cloud computing. More granular guidance would allow less flexibility to accommodate new challenges in this policy area.

Secondly, the recommendations do not include specific requirements for reporting of security incidents by institutions to their competent authorities in the context of cloud outsourcing. Since the topic of security incident reporting is broader than only for the context of cloud computing, the introduction of detailed recommendations would affect other potential security-related issues outside the regulatory scope. It is therefore more reasonable to assess the topic outside the scope of the current draft recommendations in relation to cybersecurity in general.

Furthermore, the option was taken of following a proportionate approach with regard to the requirements on the exercise by institutions of their right to audit cloud service providers. Although the right to audit needs to be contractually secured, institutions can exercise it in a proportionate manner (e.g. by organising pooled audits with other customers of the same cloud service provider) to minimise the organisational burden on both institutions and cloud service providers.

Finally, the option was taken not to include the requirement for consent of the outsourcing institutions when the cloud service provider intends to change subcontractors. This was considered overly burdensome from a practical perspective in the context of cloud outsourcing, because subcontracting is used extensively, the cloud environment is more dynamic than traditional outsourcing environments, and cloud services are provided to a larger number of clients than traditional outsourcing and on a larger scale. The option was taken to include the requirement for *ex-ante* notification of the outsourcing institutions by the cloud service providers, but not require their consent (in any case they should retain the right to terminate the contract if the planned changes of subcontractor or subcontracted services would have an adverse effect on the risk assessment of the outsourced services).

These preferred technical options are expected to give rise to less administrative costs for institutions or competent authorities. Given the ever-developing and ever-changing environment of cloud outsourcing, a less exhaustive and more flexible approach is expected to provide an optimal regulatory framework. The major benefits of this framework are that it will result in greater certainty, a reduction in operational risk, a level playing field across institutions and supervisory convergence. These benefits are expected to exceed the cost associated with compliance.

5.2 Feedback on the public consultation

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for three months, from 18 May 2017 to 18 August 2017. A total of 47 responses were received, of which 37 were published on the EBA website. The Banking Stakeholder Group did not provide an opinion.

This section presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases, several industry bodies made similar comments or the same body repeated its comments in response to different questions. In such cases, the comments and the EBA's analysis are included in the section of this paper where the EBA considers them most appropriate.

Changes to the recommendations have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

Most respondents were supportive of and positive about the EBA's initiative to provide common EU-wide guidance to institutions on outsourcing to cloud service providers and to provide clarity and convergence vis-à-vis the regulatory expectations and supervisory requirements that apply to cloud outsourcing. The respondents agreed that there is currently a high level of uncertainty regarding the supervisory expectations that apply to outsourcing to cloud service providers, which forms a barrier to the adoption of cloud solutions in the EU and to institutions realising the full benefits of cloud services.

In general, respondents supported the incorporation of the principle of proportionality in the recommendations. A number of respondents expressed concern that the recommendations would leave too much room for diverging approaches and additional requirements from competent authorities, thus not achieving the desired level of harmonisation.

More clarification was requested by respondents both on the principles underlying the materiality assessment and on the process for informing competent authorities about material cloud outsourcing. Some respondents suggested that institutions should be allowed to inform the competent authority after the contractual agreement with the cloud service provider or on an annual basis, instead of having to inform the competent authority on a case-by-case basis.

The responses emphasised that institutions have limited bargaining powers in contract negotiations with large cloud service providers. In contrast to suppliers in more traditional forms of outsourcing, cloud service providers provide standardised operations on a large scale, which may limit opportunities to negotiate changes in agreements. In this respect, respondents proposed a solution in the form of a reference framework for model contract clauses covering all regulatory

requirements or in the form of third-party certification of cloud service providers, which could assure outsourcing institutions adopting cloud services that the certified providers had met their technical and legal obligations. The criteria for such third-party certification would be developed by cloud service providers in cooperation with the financial services industry and in line with the regulatory requirements.

As regards the right to access and audit cloud service providers, respondents argued that the requirement for such full access to cloud service providers' business premises did not take account of the commercial service delivery model for cloud services, which is by design virtual and global. Cloud service providers serve numerous customers using different locations across the globe; therefore, the business model is not comparable to traditional outsourcing relationships, which are much more bespoke.

The option included in the recommendations for institutions to exercise their right to audit in a risk-based manner and make use of pooled audits and third-party certification was welcomed by respondents and deemed especially important for small and medium-sized institutions given the economies of scale. In this context, further guidance was requested with regard to the necessary qualifications of competent third-party auditors and certifiers.

Respondents also indicated that the added value of access to physical locations was rather low in cloud technology environments, where data are physically and geographically dispersed across many systems, data centres and countries. Physical access would enable only the most basic verification of physical security and access checks. Logical access to the data and a virtual audit of data would be much more relevant to ensure that the appropriate controls were in place.

In the context of the location of data and data processing, respondents emphasised that the global dimension of cloud outsourcing should be taken into account. With the technology evolving, the physical location of data becomes less easy to identify and readable data chunks are sliced, encrypted and stored across different systems worldwide. In this respect, some respondents suggested that reference should be made to the EU General Data Protection Regulation (GDPR). Industry representatives also pointed out that cloud service providers can offer customers flexibility and choice in terms of the regions and geolocations where their data is stored.

With regard to chain outsourcing, respondents pointed out that the effective monitoring of risk is more challenging in many cloud environments, given the lack of visibility of the whole supply chain of the technology stack.

Respondents agreed that robust contingency plans and exit strategies are crucial to increasing trust and resilience, and therefore to the adoption of cloud outsourcing. Testing exit strategies was deemed to be impractical and overly burdensome; therefore, alternative means of assurance, such as tabletop testing, were proposed.

A number of respondents called attention to cyber-risk as one of the major risks related to cloud outsourcing. On account of the increasing concentration of processes and data with providers, they are becoming more attractive targets for cyber-criminals. In this context, respondents asked for

further common measures, cooperation and information sharing between all stakeholders, at EU and national levels.

In the context of cyber-risk, a number of respondents asked for the recommendations to include guidance on the handling of security alerts and security incidents. Such guidance should include a requirement for cloud service providers to provide timely and complete information to institutions not only about security incidents but also about imminent threats. This would enable institutions to roll out appropriate incident prevention and containment measures. It was also suggested that explicit references should be made in the recommendations to existing regulation on security incidents and reporting.

The EBA has carefully examined all the comments received (see the table below) and has amended the text of the recommendations where appropriate.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Responses to questions in Consultation Paper EBA/CP/2017/06			
Question 1. **Are the provisions included in these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?**	A number of respondents indicated that the recommendations remained too high level and could leave room for multiple interpretations, different reporting criteria and/or fragmentation at national level.	The EBA agrees that there is a need for an EU-wide common approach to requirements in relation to cloud computing. These recommendations provide common EU-wide guidance for both institutions and supervisors and are expected to be implemented by EU competent authorities under the 'comply or explain' principle. The recommendations provide guidance on a principle-based basis, in line with the CEBS guidelines and to keep the recommendations future-proof. The EBA intends to engage with the sector and provide further guidance to assist with convergence in the implementation of the recommendations in the form of a formal Q&A process.	No changes made.
General comments			
Link with the CEBS guidelines	A few respondents pointed out that it would have been beneficial to revise the CEBS guidelines as a whole and to provide one common product. This would have had the benefit of addressing the different implementations of the CEBS guidelines and would have avoided unnecessary administrative burdens on and costs for outsourcing institutions. Furthermore, the CEBS	The EBA welcomes the proposal to clarify that the recommendations complement the existing CEBS guidelines and should be read in conjunction with those guidelines. The wording has been amended accordingly. The EBA agrees that the revision of the CEBS guidelines needs to result in one common	Paragraph 13 of the background section has been amended to clarify that the recommendations should be read in

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	guidelines were issued in 2006, and the outsourcing context and arrangements in terms of the use of technology in financial services have changed fundamentally since then. Another respondent suggested that it should be explicitly stated that the recommendations complement the existing CEBS guidelines and should be read in conjunction with those guidelines.	legal instrument on outsourcing, including cloud outsourcing. In respect of the timeline for the review of the CEBS guidelines, it was decided to issue these recommendations early in view of the urgency of the need for common guidance on cloud outsourcing. We would like to clarify that these recommendations will feed into the review of the CEBS guidelines in order to combine all outsourcing requirements in one policy product.	conjunction with the CEBS guidelines.
Harmonisation of international frameworks on cloud outsourcing	One respondent emphasised the need to create a harmonised global technology risk framework, as divergent practices across jurisdictions form a barrier to the adoption of cloud services. The respondent encouraged for the development of best practices, industry standards and third-party certifications by the industry in cooperation with the regulated firms.	The EBA welcomes the suggestion of the creation of a harmonised global technology risk framework. The EBA also acknowledges the need for harmonised practices across jurisdictions, both within and outside of the EU. Whereas these recommendations are an initiative to harmonise requirements at EU level, the EBA is also involved in the work of international bodies on this topic.	No changes made.
Use of recommendations as policy instrument	A few respondents indicated that the use of recommendations for cloud outsourcing, which are by nature not directly applicable or mandatory, could introduce an element of divergence and differences in application. The use of technical standards or any other mandatory instrument would be a better option to bring about harmonisation.	There is no specific mandate in European legislation to draft and adopt binding technical standards on cloud outsourcing; therefore, these recommendations were developed as an 'own initiative regulatory product' by the EBA pursuant to Article 16 of the EBA Regulation, subject to the 'comply or explain' principle.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Principle of proportionality	One respondent proposed that the recommendations should explicitly allow for proportionality depending on the risk profile of the service managed by the cloud service provider.	As stated in the executive summary, the principle of proportionality applies throughout the recommendations, which should be employed in a manner proportionate to the size, structure and operational environment of the institution, as well as the nature, scale and complexity of its activities.	No changes made.
Granularity of the recommendations	Several respondents requested that the recommendations be more granular, providing specific guidance on different types of cloud service models.	The recommendations were designed to be technology-neutral and future-proof as well as principle-based in line with the CEBS guidelines. In view of the many different possible combinations of service/deployment models and the constant evolution of cloud service models, it would not be feasible to provide more granular guidance in this respect.	No changes made.
2. Subject matter, scope and definitions			
Subject matter			
Scope	One respondent pointed out that, whereas the CEBS guidelines apply to 'credit institutions', the draft recommendations, which build on the CEBS guidelines, apply to institutions as defined in Article 4(1) of the CRR, thus including certain investment firms.	The EBA wishes to clarify that the scope of the recommendations includes institutions as defined in point 3 of Article 4(1) of the CRR, covering both credit institutions and investment firms. A similar approach to that of the CEBS guidelines was taken. In relation to institutions offering investment services, an	Paragraph 14 has been added to the background section to clarify the application of the recommendations to investment firms. The wording

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		analysis was performed to ensure that these recommendations are fully consistent with the relevant provisions of MiFID II on outsourcing and the related implementing regulation.	of paragraph 3 of the executive summary has been amended accordingly.
Scope	A few respondents requested that the EBA clarify if the recommendations apply to material cloud services only, or at least that it clarify which provisions apply only to material cloud services and which apply also to non-material cloud services.	The EBA wishes to clarify that all the provisions in the recommendations apply to both material and non-material cloud outsourcing. The only exception is the duty to inform the competent authority under paragraphs 2 and 3, which applies only to material cloud outsourcing.	No changes made.
Scope	A few respondents proposed clarifying in the recommendations that they apply only to activities relating to the provision of regulated financial services. All other functions, such as HR, supporting functions (e.g. legal services) and functions relating to other business areas (e.g. mobility, health care), that may be provided by a financial institution (or a company belonging to the same group as a financial institution) should be outside the scope of these recommendations. One respondent suggested using different levels of cloud outsourcing to clarify which types of activities are considered cloud outsourcing for the purposes of these recommendations.	The EBA wishes to clarify that the recommendations apply to all functions and activities of institutions, so both regulated services and all services that support those services are within the scope of these recommendations. The proposed classification of outsourcing levels is not deemed to be practical in the context of the recommendations.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Scope	One respondent suggested to that it should be perfectly clear that neither these EBA recommendations, nor any EU supervisory framework applies to cloud outsourcing by financial institutions that are not subject to the EU supervisory framework even though the parent company is under it.	The EBA wishes to clarify that the recommendations will apply only to EU credit institutions and investment firms.	No changes made.
Scope	A few respondents requested that the recommendations refer to 'cloud computing services' rather than 'outsourcing to cloud service providers.' These respondents emphasised that cloud services should not all be considered 'outsourced' services under the CEBS guidelines, as some can be classified as 'purchasing' in accordance with the definition in the CEBS guidelines. The purchasing of server capacity, for example, should be classified as 'purchasing of cloud computing products'.	The definition of cloud computing used in these recommendations is covering the general understanding of competent authorities about what cloud computing is within an outsourcing context. The EBA's view is that the definitions of outsourcing and cloud computing are sufficient.	No changes made.
Definitions	A few respondents indicated that the EBA's definition of cloud services is more concise than the definition of the National Institute of Standards and Technology (NIST). One respondent suggested using the full NIST definition of hybrid cloud to increase the clarity of the definition.	The current definitions of cloud services and hybrid cloud are deemed to be sufficiently clear.	No changes made.
Definitions	A few respondents indicated that, whereas the NIST definition has been used to define cloud services, the NIST definitions have not been used for cloud service models (SaaS, IaaS and PaaS).	The EBA agrees with the concern that service models are constantly evolving and has removed the references to SaaS, IaaS and PaaS (and the related definitions) and	The definitions of SaaS, IaaS and PaaS were removed from the definitions

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Furthermore, a number of respondents pointed out that the service models are constantly evolving and that therefore references to specific cloud service models are not future-proof.	replaced this text with a more generic reference to 'cloud service models'.	section, and paragraph 5(b) amended to refer to 'cloud service models' in general.
Definitions	One respondent proposed including a definition of multi-tenant service provider in view of the reference in section 4.3 (access and audit rights).	The concept of a multi-tenant cloud environment offering cloud computing functions to a number of different clients, as also explained in paragraph 8 of the background section, is deemed to be sufficiently clear.	No changes made.
4.1 Materiality assessment			
4.1 Materiality assessment – Paragraph 1 – References to CEBS guidelines	One respondent proposed including a specific reference to the relevant principles of the CEBS guidelines in the context of the materiality assessment.	The EBA agrees with the suggestion to clarify which principles of the CEBS guidelines are referred to in the context of the materiality assessment and has amended the wording accordingly.	Paragraph 1 has been amended to include a reference to guideline 1(f) of the CEBS guidelines.
4.1 Materiality assessment – Qualitative and quantitative assessment criteria	Several respondents suggested providing more detailed qualitative or quantitative criteria to objectively establish if a service is considered material cloud outsourcing or not. This should ensure the consistent application of the materiality assessment. In this respect, it was also proposed that a list of non-exhaustive examples and exclusions in relation to material outsourcing be included.	The EBA welcomes the suggestion and wishes to explain that, in line with the principle-based approach and to keep the recommendations future-proof, no further qualitative or quantitative criteria for the materiality assessment are to be included. The EBA proposes to provide advice on a more continuous basis after the publication of the recommendations in the form of a Q&A sharing specific examples of what is regarded	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	It was also suggested that material cloud outsourcing be limited to core business with reference to Annex 1 to Directive 2013/36/EU, 'List of activities subject to mutual recognition'.	as material outsourcing in view of new developments, thus assisting further convergence. The EBA wishes to clarify that the materiality assessment should not be limited only to regulated activities.	
4.1 Materiality assessment – Repeat assessments	A few respondents suggested allowing the possibility of avoiding duplicate materiality assessments where activities are identical or very similar, by allowing outsourcing institutions to rely on previous similar assessments.	The recommendations allow institutions the flexibility to build on previous assessments in the case of very similar new cloud outsourcing activities.	No changes made.
4.1 Materiality assessment – Application of new requirements	One respondent asked whether the existing materiality assessments covering technology outsourcing in line with the requirements of the national competent authority will need to be amended to bring them in line with the guidance in these recommendations.	The EBA wishes to clarify that the guidance on the materiality assessments will apply as from the application date for any new cloud outsourcing arrangements or revisions of materiality assessments for existing arrangements as from that date.	No changes made.
4.1 Materiality assessment – Risk appetite	One respondent requested clarification in the recommendations that banks remain responsible for setting their own risk appetites and that increased risks in some areas may be acceptable if the overall risk to the institution is lower as a result of the outsourcing.	The EBA agrees that institutions remain responsible for setting their own risk appetites, as required by Article 76 of Directive 2013/36/EU and paragraph 23(b) of the EBA Guidelines on internal governance (EBA/GL/2017/11).	No changes made.
4.1 Materiality assessment – Standalone basis	One respondent suggested that the recommendations should clearly establish that materiality needs to be assessed on a standalone	The EBA wishes to clarify that the recommendations, including on the materiality assessment in section 4.1, apply	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	basis, by entity, not at a group level. Each subsidiary should perform its materiality assessments.	at the level of the entities indicated in the scope.	
4.1 Materiality assessment – Assessment criteria - paragraph 1(a)	A few respondents suggested that the materiality assessment should focus on the closeness of the connection between the cloud technology service and the critical or important function it supports. Where the connection is such that the use of the technology could have a material impact on the institution's ability to continue to perform the activity in question, it should be considered material.	The EBA acknowledges the importance of the criticality of the service supported by the cloud service for the determination of materiality. This aspect is deemed to be sufficiently covered by assessment principle 1(a), which refers to the criticality and inherent risk profile of the activities to be outsourced, i.e. are they activities that are critical to the business continuity/viability of the institution and its obligations to customers.	No changes made.
4.1 Materiality assessment – Assessment criteria – paragraph 1(b)	A few respondents suggested removing the assessment criterion based on the direct operational impact of outages, as it incorrectly assumes that the risk of disruption would increase with the use of cloud services.	The EBA wishes to clarify that it not assumed that the risk of disruption would always increase with the use of a cloud service provider. However, the impact of potential outages is to be taken into account by the outsourcing institution when assessing the materiality of the outsourced activity.	No changes made.
4.1 Materiality assessment – Assessment criteria – paragraph 1(c)	A few respondents requested to delete assessment principle 1 (c) related to the impact of the disruption on the revenue prospects since it cannot be allocated to a single outsourcing.	The EBA notes the comment and wishes to clarify that the assessment principle has been included because it refers to significant disruption in the short term.	No changes made.
4.1 Materiality assessment – Assessment criteria – paragraph 1(d)	A few respondents suggested the deletion of assessment principle 1(d) on the potential impact of a breach of confidentiality or data integrity failure, since this has to be assessed for any service	The EBA wishes to clarify that the aspect of the confidentiality and integrity of data is deemed to be an important element in the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	regardless of whether it is outsourced. Furthermore, this is already covered by existing data protection regulation. One respondent proposed rephrasing assessment principles 1(b), (c) and (d) to refer to 'likelihood' and potential impact.	assessment of the materiality of cloud outsourcing activities. The EBA notes the comment about the inclusion of 'likelihood'. However, the current wording of principles 1(b), (c), and (d) makes reference to the inherent risk not the residual risk.	
4.2 Duty to adequately inform supervisors			
4.2 Duty to adequately inform supervisors – Material outsourcing versus material cloud outsourcing information	One respondent requested further clarification regarding the interplay between notifications for material outsourcing and notifications for material cloud outsourcing, since the existing material outsourcing notifications are likely to cover cloud outsourcing as well.	The EBA welcomes the comment and agrees that it will be necessary to avoid unnecessary duplication in the information for material outsourcing and for material cloud outsourcing. The EBA wishes to clarify that it is expected for the information to competent authorities on material cloud outsourcing to be brought in line with these recommendations.	No changes made.
4.2 Duty to adequately inform supervisors – Duplication of information requirements	A few respondents pointed out a duplication in the form and content of the information to be collected and reported to competent authorities. This duplication is increased by the ability of competent authorities to request additional information.	Although the recommendations take a multi-level approach to information requirements, there should be no duplication between the different levels of information. Competent authorities always retain the right to request ad hoc additional information. In this regard, it was intended to predefine and harmonise such additional information requests by including the list in paragraph 3, although the list is not exhaustive.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.2 Duty to adequately inform supervisors – *ex ante/ex post*	Several respondents requested further clarification regarding the timing (before or after outsourcing) in relation to the duty to adequately inform the supervisor about material cloud outsourcing, since the timing requirements are not harmonised at EU level. A few respondents pointed out that the communication of contractual agreements with cloud service providers once signed, and the security policy and criteria agreed by the outsourcing institution and the cloud service provider, should be sufficient. It was also requested that, once the competent authority has reviewed and validated the underlying conditions and obligations, it should not be necessary to notify the provision of any service within this already assessed contract.	With regard to the timing of informing competent authorities about material cloud outsourcing, the recommendations need to stay in line with the CEBS guidelines. In this respect, it has been clarified in the recommendations that institutions should provide *ex ante* information to the competent authority about new material cloud outsourcing. The EBA notes the comment about repetitive information on minor changes within an existing cloud outsourcing framework. The EBA would like to point out the need for completeness in the information process.	Section 4.2 has been amended to clarify that the duty to adequately inform supervisors relates to material activities and data that are 'to be outsourced' to cloud service providers.
4.2 Duty to adequately inform supervisors – Format for submission of information	Several respondents asked whether a standard form or template should be used by institutions to inform their supervisor about material cloud outsourcing.	In line with the CEBS guidelines, no common template is provided at this stage for outsourcing institutions to inform their competent authority about material cloud outsourcing.	No changes made.
4.2 Duty to adequately inform supervisors – Approval of material cloud outsourcing by competent authorities	A few respondents requested clarification of whether material cloud outsourcing would be subject to prior authorisation or *nihil obstat* from the competent authority and what would be the maximum term for such pre-authorisation/*nihil obstat*.	The EBA wishes to clarify that, in line with the CEBS guidelines, the information should be made available in a timely manner to allow the competent authority to consider whether the proposal raises prudential concern and take appropriate action if required.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.2 Duty to adequately inform supervisors – Applicability to legacy contracts	One respondent proposed that the EBA provide further explanation on effective dates for legacy contracts.	The EBA wishes to clarify that these recommendations will apply as from the application date for any new materiality assessments or revisions of materiality assessments undertaken as from that date.	No changes made.
4.2 Duty to adequately inform supervisors – Case-by-case submission of information	A number of respondents pointed out that case-by-case information of material cloud outsourcing to the competent authorities would increase the time to market and is not the most efficient approach.	In line with the CEBS guidelines, the case-by-case notification is maintained for material cloud outsourcing.	No changes made.
4.2 Paragraph 2(a) – Name of the cloud service provider and parent company	One respondent asked for clarification of what 'parent company' refers to in the requirement for outsourcing institutions to inform competent authorities about the name of the cloud service provider and the name of the parent company. Another respondent suggested including full information regarding the ownership structure and ultimate/beneficial owner(s) of the cloud service provider in the information to be provided to competent authorities.	The EBA wishes to clarify that the parent company as mentioned in paragraph 2(a) refers to the company that owns or controls the cloud service provider by owning an influential amount of voting stock or control. The recommendations do not require outsourcing institutions to provide information about the ownership structure of the cloud service provider other than the name of the parent company (if applicable).	No changes made.
4.2 Paragraph 2(c) – Country where the service is performed (including location of data)	Several respondents indicated that the location of data in the case of cloud outsourcing can refer to multiple countries where support, data centres and backup services are located. Furthermore, data in transit may pass through a number of different countries. It was also mentioned that, although cloud service providers can specify where data are stored and	The EBA welcomes the suggestion and agrees to reflect the potential multiple locations of data in the text. The EBA would also like to clarify that the location of data refers to the jurisdiction rather than the exact address of the location. The country where the service is performed and the location where data are stored are	Paragraph 2(c) has been amended to refer to the country or countries where the service is to be performed (including the location of data) as part of the

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	processed and where they have operations, it is not easy for them to specify where a service is actually performed. One respondent pointed out that the reference to the location of the data could be interpreted as requiring a more precise location (e.g. an address), which for security purposes would be sensitive information.	deemed important information for the competent authority in view of transparency, the supervisory dialogue and supervisory access to these data.	information to be provided to competent authorities with regard to material cloud outsourcing.
4.2 Paragraph 2(g) – Service expiry or next contract renewal date	One respondent pointed out that many cloud service agreements do not have a fixed expiry or renewal date and that they remain in force until terminated.	The EBA welcomes the comment and agrees that the expiry or renewal date of the contract should be provided to the competent authority only where relevant.	Paragraph 2(g) has been amended to state that the service expiry or next contract renewal date should be provided 'where applicable.'
4.2 Paragraph 3 – Additional information for competent authorities	One respondent suggested that the requirement for additional information on material cloud outsourcing to be kept at the disposal of the competent authority is superfluous given the powers of competent authorities to require information and documents from regulated firms.	The EBA agrees with the comment that competent authorities have the power to require information and documents from regulated firms. In this regard, it was intended to predefine and harmonise such additional information requests by including the list in paragraph 3, although the list is not exhaustive.	No changes made.
4.2 Paragraph 3(a) – Business continuity plan of the cloud service provider	Several respondents indicated that it is unclear whether it is sufficient for outsourcing institutions to be able to confirm the existence of a business continuity plan of the cloud service provider or if	The EBA welcomes the comment and wishes to clarify that the current wording of paragraph 3(a) refers to the existence of a	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	they would need to confirm the details of the plan. Respondents also asked whether the competent authority needs to approve the business plan.	business continuity plan rather than to the details of the plan. As detailed at the start of paragraph 3, the information on this information is part of the additional information competent authorities may request be included in the risk assessment by the outsourcing institution of the material activities outsourced. It is not required for the business continuity plan of the cloud service provider to be communicated to the competent authority, nor does the competent authority need to approve this plan.	
4.2 Paragraph 3(c) – Skills and resources retained by the outsourcing institution to monitor the outsourced activities	A few respondents indicated uncertainty about what constitutes the necessary skills and resources that the outsourcing institution must have to adequately monitor the outsourced activities.	Institutions are allowed sufficient flexibility to decide what constitutes the necessary skills for their particular cloud outsourcing, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	No changes made.
4.2 Paragraph 4 – Register of information on outsourced activities – Scope: cloud outsourcing	A number of respondents pointed out that the requirement for institutions to maintain a register for all their material and non-material outsourced activities was not limited to cloud outsourcing and formed an addition to the CEBS guidelines. Another respondent suggested that there should be a transitional period for compliance, since that level of register recording has not previously been required (i.e. for non-material activities).	The EBA welcomes the suggestion and agrees that the requirement for outsourcing institutions to maintain a register of outsourced activities should apply only to cloud outsourcing in the context of these recommendations. Since the requirement to maintain a register will apply only to cloud outsourcing in the context of these recommendations, an	Paragraph 4 has been amended such that the register is to be maintained only for 'cloud' outsourcing.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	One respondent asked what the purpose of such a register would be from the point of view of the competent authorities.	additional transitional period for compliance is not deemed necessary. The EBA wishes to clarify that the information from the register might be used for several purposes by the competent authorities, inter alia for the monitoring of the concentration risk.	
4.2 Paragraph 4 – Register of information on outsourced activities – Inclusion of existing cloud outsourcing agreements	A few respondents would welcome some clarification regarding whether this new register is to be created exclusively for the purpose of outsourcing cloud services and whether existing outsourcing services will not be concerned until the contract is renewed.	The EBA wishes to clarify that the requirements with regards to the register will apply as from the application date for any new cloud outsourcing agreements or revisions of existing agreements as from that date. For institutions that do not yet have a centralized outsourcing register in place which also covers cloud outsourcing, it is suggested to consolidate the cloud outsourcing information and complete the register. This would allow the institution to centralize all information needed to assess the risk of the cloud outsourcing and how it is managed by the institution. Where institutions already have a register for outsourcing, the information on cloud outsourcing can be included in the existing register and no separate register needs be created for cloud outsourcing.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.2 Paragraph 4 – Register of information on outsourced activities – At group/entity level	Several respondents requested that the EBA allow sufficient flexibility for outsourcing institutions to keep the outsourcing register at group level or at the level of the individual legal entities. One respondent requested that the EBA clarify that the register should be kept only by European banking groups at European level, as such a provision might not exist in third countries.	The EBA wishes to clarify that the requirement to maintain the register applies at institution and group levels, although only for the European entities of the group. This will allow monitoring of the concentration risk.	No changes made.
4.2 Paragraph 4 – Register of information on outsourced activities – Material/non-material cloud outsourcing	A number of respondents proposed limiting the register to material cloud services only or including some form of proportionality in the requirement for institutions to maintain a register of information on their outsourced activities. One respondent proposed setting a threshold below which cloud outsourcing is not required to be reported to regulators and is exempt from the requirements in paragraph 5. A few respondents suggested rephrasing the requirement for institutions to maintain a register on their outsourced activities to avoid the explicit specification of a list of minimum required information.	The EBA notes that the overall principle of proportionality applies throughout the recommendations, which should be applied in a manner proportionate to the size, structure and operational environment of the institution, as well as the nature, scale and complexity of its activities. The EBA would like to clarify that the requirement for institutions to adequately inform their competent authorities applies only to material cloud outsourcing. For non-material cloud outsourcing activities, institutions need to have the information referred to in paragraph 5 available, but this information is not to be reported to the competent authorities. The EBA wishes to explain that the purpose of this requirement was to include a minimum rather than a maximum list of information to be kept in the outsourcing register. As the register is mainly for the internal use of	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		institutions, the aim was to avoid restricting the type of information that can be contained in it.	
4.2 Paragraph 4 – Register of information on outsourced activities – Inclusion of contracts	One respondent requested that the EBA clarify whether outsourcing contracts, regardless of the materiality of the underlying cloud outsourcing, should be included in the register or not.	The EBA would like to clarify that, although centralising all outsourcing contracts provides an overview and makes it easier to handle, implement and control a change in materiality, it is not part of the requirement under paragraph 5 for the register to include all cloud outsourcing contracts.	No changes made.
4.2 Paragraph 5 – Register of information on outsourced activities (b) – Type of outsourcing	Several respondents indicated that the reference to examples of cloud service models (SaaS, IaaS and PaaS) does not appear to be technology-neutral. The respondents pointed out that these terms are likely to change or disappear over time and that there exists almost limitless variation in service models.	The EBA agrees that service models are constantly evolving and has removed the references to SaaS, IaaS and PaaS (and the related definitions) and replaced the text with a more generic reference to 'cloud service models'. The reference to cloud deployment models has been retained, as, together with cloud service models, they are an important factor in the risk assessment of cloud outsourcing.	Paragraph 5(b) has been amended to refer to 'cloud service models' in general instead of listing examples.
4.2 Paragraph 5 – Register of information on outsourced activities (c) – Parties receiving cloud services	A few respondents suggested that it is not clear who the 'parties' receiving the cloud services referred to in paragraph 5(c) might be.	The EBA wishes to clarify that paragraph 5(c) refers to the entities of the group or other parties receiving cloud outsourcing services.	No changes made.
4.2 Paragraph 5 – Register of information on outsourced	A few respondents indicated that cloud outsourcing is not necessarily approved by the management body or a committee designated by	The purpose of the requirement under paragraph 5(c) is to ensure that outsourcing institutions have appropriate internal	Paragraph 5(d) has been amended to reflect that

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
activities (d) – Management body approval for outsourcing	it, as it can also be approved at other levels, depending on the type of outsourcing, its materiality, etc.	governance around decisions on cloud outsourcing, in particular if it is considered material.	information should be provided about the approval for the cloud outsourcing by the management body or its delegated committees, if applicable.
4.2 Paragraph 5 – Register of information on outsourced activities (e) – Main subcontractor	Several respondents requested clarification of the meaning of 'main subcontractor' in paragraph 5(e).	The EBA welcomes the comment and has amended the wording to specify that the names of any subcontractors (if applicable) are to be included in the cloud outsourcing register.	Paragraph 5(e) has been amended to clarify that the names of any subcontractors are to be included in the cloud outsourcing register.
4.2 Paragraph 5 – Register of information on outsourced activities (h) – Date of last materiality assessment	A few respondents asked for clarification of the frequency with which outsourcing institutions should review their materiality assessments for cloud outsourcing.	The EBA wishes to clarify that the recommendations do not prescribe any specific requirements in terms of the frequency for the review of materiality assessments for cloud outsourcing, to allow institutions sufficient flexibility to determine this in view of their specific requirements, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.2 Paragraph 5 – Register of information on outsourced activities (i) – Time-critical business operations	Several respondents suggested including further clarification of what is meant by 'time-critical' business operations that are supported by the cloud service provider or significant subcontractor and of what is meant by 'significant subcontractor'.	The EBA clarifies that time-critical business operations refer to those business operations that have been defined in the outsourcing institution's own risk assessment as time critical (in terms of RTO, RPO, etc.). The EBA welcomes the comment on the reference to 'significant' subcontractors and has amended the wording and aligned it with paragraph 5(e).	Paragraph 5(i) has been amended to remove the reference to 'significant' subcontractors.
4.2 Paragraph 5 – Register of information on outsourced activities (j) – Assessment of the cloud service provider's substitutability	Several respondents suggested following a time-based approach to the assessment of the substitutability of cloud service providers, rather than classifying them according to the degree of ease of substitution. One respondent requested clarification of the term 'substitutability' of the cloud service provider. Another respondent suggested removing an assessment of the cloud service provider's substitutability from the requirements for information to be kept in the register, as it results in a duplication of the requirements for the exit strategy.	The EBA agrees that the time needed to substitute the cloud service provider is an important element linked to the assessment of the degree of ease or difficulty with which the provider can be substituted. However, the time component is not the only element that determines substitutability, and ultimately the assessment remains at the discretion of the outsourcing institution. The term 'substitutability' refers to the ease and speed with which the outsourcing institution can change from one cloud service provider to another for a particular service or activity. The EBA would like to clarify that, whereas the assessment of substitutability will form part of the exit strategy, the outcome of it, or at least the fact that a substitutability	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		assessment took place, should be recorded in the outsourcing register.	
4.2 Paragraph 5 – Register of information on outsourced activities (l) – Due diligence on outsourcing or subcontracting arrangements	Several respondents requested that the EBA clarify what is meant by 'due diligence on outsourcing or subcontracting arrangements'. A few respondents asked the EBA to provide clarification regarding the minimum frequency with which the regular due diligence on outsourcing or subcontracting arrangements needs to be performed.	The EBA welcomes the comment and has amended the wording to reflect that outsourcing institutions should include the date of the last risk assessment of the outsourcing or subcontracting arrangements in the cloud outsourcing register. The recommendations do not prescribe any specific requirements in terms of the frequency of the review of the risk assessment of outsourcing or subcontracting arrangements to allow institutions sufficient flexibility to determine this in view of their specific requirements, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	Paragraph 5(l) has been amended to clarify that outsourcing institutions should include the date of the last risk assessment in the cloud outsourcing register.
4.3 Access and audit rights			
Access and audit rights for institutions			
4.3 Access and audit rights – Paragraphs 6 to 14 – Proportionality	One respondent suggested that the principle of proportionality be observed by institutions in determining the extent to which audit rights must be provided.	Although the principle of proportionality applies throughout the recommendations, it should be noted that the rights to audit and access should always be ensured contractually, regardless of the level of use of the cloud services. As provided for in the recommendations, the exercise of these	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		rights can be done in a risk-based manner by the outsourcing institution.	
4.3 Access and audit rights – Paragraphs 6 to 14 – Feasibility of full access/audit	A number of respondents considered the full rights to access and audit for outsourcing institutions infeasible in view of highly standardised services and contracts, the limited negotiation power of outsourcing institutions, the risk these rights pose to the cloud environments of other clients and the security risk and operational implications for the cloud service provider as a whole. Respondents also pointed out that the added value of physical facility access can be considered extremely low in modern-day technology environments, where data are physically and geographically dispersed across many systems, data centres and even countries.	The EBA notes the comments with regard to the feasibility of the full rights of access and audit and would like to reiterate that, although these rights should be contractually assured, they can be exercised in a risk-based manner. Since the outsourcing institution retains responsibility for the outsourced functions, it is vital for the institution to have the necessary access and audit rights to fulfil its obligations.	No changes made.
4.3 Access and audit rights – Paragraphs 6 to 14 – Feasibility of full access/audit – Proposed alternatives	Several respondents suggested alternative solutions to the access and audit rights for outsourcing institutions to cloud service providers. Some respondents proposed allowing financial institutions to leverage existing industry standards and certifications of cloud service providers, or third-party certification recognised by the competent authorities. Other respondents pointed out that virtual access to systems and data should be considered sufficient.	The EBA notes the proposed alternatives to the access and audit rights for outsourcing institutions and would like to clarify that, although the access and audit rights should be ensured contractually, outsourcing institutions have the flexibility to exercise these rights in a risk-based manner (e.g. by relying on third-party audit reports or certifications). The EBA wishes to clarify that virtual/logical access is deemed to be de facto included in the audit tools both for institutions and competent authorities. In addition to physical	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Another suggestion made, in the context of multi-tenant cloud environments, was applying pooled customer audits or third-party audit reports or certifications and limiting direct access and audit rights of institutions to cloud service providers to exceptional cases when external audit reports do not comply with applicable audit report standards or when shortcomings or other issues are detected.	access to the business premises of the cloud service provider, right of access also refers to the 'full range of devices, systems, networks and data' used to provide the services outsourced. Although the option of organising pooled audits is specified as one of the ways in which institutions can exercise their right to audit, the intention was to retain flexibility for the outsourcing institutions in this respect and not to impose the use of pooled audits in the context of multi-tenant cloud environments.	
4.3 Access and audit rights – Paragraph 6 – Written agreement	One respondent pointed out that the vast majority of agreements for cloud services are concluded online via electronic acceptance of standardised terms and conditions. The respondent proposed explicitly referring to electronically concluded agreements in the recommendations.	The EBA welcomes the comment and wishes to clarify that the term 'written agreement' is understood to cover agreements that are in electronic format.	No changes made.
4.3 Access and audit rights – Paragraph 6(a) – Access to business premises of the cloud service provider for outsourcing institutions or 'any third party'	A number of respondents indicated that the requirement to include in the cloud outsourcing agreement the right of access for the institution and 'any' third party appointed by the institution or by the competent authority appears to be too broad.	The EBA wishes to clarify that the reference to 'any third party' is deemed to be sufficiently qualified in paragraph 9, which requires that third parties acting for the outsourcing institution should have the appropriate skills and knowledge to perform effective and relevant audit assessments of the cloud solutions.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.3 Access and audit rights – Paragraph 6(a) – Access to business premises	Several respondents indicated that access to the cloud service provider's business premises for outsourcing institutions should be limited to the business premises that are actually used to provide the service to the outsourcing institution, taking into account practical, security and confidentiality concerns in multi-tenant cloud environments. A few respondents asked for clarification of whether access to business premises includes access to data centres. It was also suggested that data centres be explicitly excluded from the right of access or that cloud service providers should be able to limit access to data centres for security reasons.	The EBA welcomes the suggestion and has amended the wording to clarify that access should be provided to the business premises, including the full range of devices, systems, networks and data, that are actually used for providing the services outsourced. The EBA clarifies that access to business premises (head offices and operations centres), which needs to be contractually ensured, should include access to data centres.	Paragraph 6(a) has been amended to clarify that access is required to the business premises (head offices and operations centres), including the full range of devices, systems, networks and data 'used for providing the services outsourced.'
4.3 Access and audit rights for institutions – Paragraph 7 – Impediments to the effective exercise of the rights of access and audit	A few respondents pointed out that a common limitation imposed in contracts with cloud service providers is a limitation on the number of audit rights per year. The respondents requested that the EBA clarify that such limitations are considered an impediment to the rights of access and audit. The respondents also indicated that contracts with cloud service providers often include the right of the cloud service provider to impose charges in relation to the requirement to cooperate with competent authorities and on institutions and their auditors for an onsite visit.	The EBA welcomes the comment and agrees that there should be no contractual limitations to the outsourcing institution's right to audit. The EBA notes the remark about the contractual clauses imposing charges on outsourcing institutions for the cooperation by cloud services providers with competent authorities and on institutions and their auditors for onsite visits. These would fall under the contractual arrangements between the outsourcing institution and the cloud service provider.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.3 Access and audit rights for institutions – Paragraph 7 – Risk to another client's environment	A few respondents requested guidance on what the EBA considers 'alternative ways' to provide a similar level of assurance. A few respondents proposed complementing the requirement to take into account the risk to another client's environment when performing audits with a requirement to take into account the potential risk to the cloud service provider's own business environment.	The EBA wishes to clarify that outsourcing institutions and cloud service providers should have the flexibility to agree on alternative ways to provide a similar level of assurance if certain audit techniques might create a risk for another client's environment. A number of possible tools can be found under paragraph 8 (pooled audits, third-party certification, third-party or internal audit reports made available by the cloud service provider under the conditions indicated in paragraphs 8(b)(i–v) and 9). The EBA wants to explain that the protection applies not only to the environments of other clients, but to all other environments as well.	No changes made.
4.3 Access and audit rights for institutions – Paragraph 8 – Exercise of audit right in a risk-based manner	One respondent suggested clarifying that the term 'where an outsourcing institution does not employ its own audit resources' is intended to mean 'where an outsourcing institution chooses not to employ its own audit resources', in order to clarify that institutions that do have the necessary audit resources are not prevented from using this optionality.	The EBA wishes to clarify that the wording 'where an outsourcing institution does not employ its own audit resources' refers to both where an institution has the resources available but chooses not to employ them and where an institution does not have the resources and therefore cannot employ them.	No changes made.
4.3 Access and audit rights for institutions – Paragraph 8(a) – Pooled audits	Although respondents generally welcomed the option to use pooled audits as an alternative to institutions using their own audit resources, a few respondents asked for further clarification	The EBA would like to clarify that no hierarchical order is reflected in the order of the alternative tools for institutions to exercise their audit rights as set out in paragraph 8.	Paragraph 8(a) has been amended to state that pooled audits can be organised by the outsourcing

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	regarding the practical implementation of such audits. One respondent proposed allowing for pooled audits but as an option to be considered when other alternative solutions are not possible. Another suggestion was to reverse the order of pooled audits in paragraph 8(a) and third-party certification/audit reports in paragraph 8(b) as alternative tools for institutions to exercise their right to audit. It was also proposed that pooled audits should be organised by the cloud service providers, not by the outsourcing institutions. One respondent suggested specifying in the recommendations that pooled audits can be executed either by one of the participating outsourcing institutions or by a trusted third party.	The EBA wishes to clarify that pooled audits are a different tool from certifications or third-party audit reports provided by the cloud service provider, in that they are organised by the customers themselves. The EBA welcomes the suggestion to clarify that pooled audits can also be performed by a third party designated by the outsourcing institutions that form the pool and has amended the wording accordingly.	institutions or by a third party appointed by them.
4.3 Access and audit rights for institutions – Paragraph 8(b)(i) – Third-party certification/audit reports – Covering key systems and controls	One respondent proposed clarifying that third-party certifications or audit reports should be relevant to the institution's use of the services and the related controls.	The EBA wishes to clarify that third-party certification or audit reports used by outsourcing institutions should cover the systems and controls identified as key by the outsourcing institution.	Paragraph 8(b) has been amended to clarify that the scope of the certification or audit reports should cover the systems and controls identified as key by the outsourcing institution.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.3 Access and audit rights for institutions – Paragraph 8(b)(ii) – Continuous assessment of third-party certification/audit reports	A few respondents suggested removing or rephrasing the requirement for outsourcing institutions to 'continuously' assess the content of the certifications or audit reports.	The EBA wishes to clarify that it is deemed important to ensure the continuous coverage of the certifications or audit reports. The aim of the wording in this paragraph is to ensure that outsourcing institutions verify on a regular basis that the scope of the certifications or audit reports on which they rely is still sufficient. The wording has been amended accordingly.	Paragraph 8(b)(ii) has been amended to clarify that outsourcing institutions should assess the content of certifications or audit reports 'on an ongoing basis'.
4.3 Access and audit rights for institutions – Paragraph 8(b)(iii) – Third-party certification – Aptitude of the certifying party	One respondent argued that the rotation of a certifying or auditing company is not an appropriate example of a way to assess the aptitude of the auditing party, especially in view of the complexity of certifying/auditing cloud services, and suggested removing this example.	The EBA acknowledges the remark about the complexity of certifying or auditing cloud services. In terms of the aptitude of the certifying or auditing party, rotation has been included as an example since it is deemed important for safeguarding the independence of the audits or certifications.	No changes made.
4.3 Access and audit rights for institutions – Paragraph 8(b)(iv) – Third-party certification/audits against widely recognised standards	Several respondents suggested that the EBA list those certifications and combinations of certifications that are deemed acceptable. One respondent requested further guidance on which core measures should be fulfilled for the use of certifications. For example, would a standard that can be fulfilled by self-assessment qualify as a recognised standard?	The EBA agrees about the need for standardisation and authorisation of certifications of cloud service providers. However, the recommendations are intended to provide flexibility for institutions to use the certifications they deem acceptable under the conditions described in paragraph 8(b). The EBA wishes to clarify that certification should be provided by an independent third party and cannot be fulfilled by self-assessment in this context.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.3 Access and audit rights for institutions – Paragraph 8(b)(v) Third-party certification – Request for modifications to the scope of the certification/audit reports	A few respondents proposed removing the requirement for outsourcing institutions to have the contractual right to request the expansion of the scope of third-party certification or audit reports, as unlimited scope expansions could prove to be a blocking issue during contractual negotiations.	The EBA wishes to clarify that the current wording does not allow for unlimited requests for scope modifications, as it is stated that they should be reasonable, and legitimate from a risk-management perspective.	No changes made.
4.3 Access and audit rights for institutions – Paragraph 9 – Audit staff skills and knowledge	A few respondents requested that the requirement on the appropriate skills and knowledge for audit staff be clarified. One respondent proposed that the verification of the appropriate skills and knowledge of the third-party auditors acting on behalf of the cloud service provider should be performed by the cloud service provider itself.	The EBA wishes to clarify that the responsibility for verifying the expertise of the third-party auditors appointed by the cloud service provider remains with the outsourcing institution if the institution wishes to rely on audit reports or certifications provided by these third-party auditors.	No changes made.
Access and audit rights for competent authorities			
4.3 Access and audit rights for competent authorities – Paragraph 10	One respondent suggested clarifying that 'business premises' is not intended to mean 'data centres.' It was also suggested to add the right to access "other relevant offices" or "relevant business centres" so that there is no restriction to head offices and operation centres. One respondent proposed rephrasing paragraph 10 to make it clear that the right of access for the competent authority applies only to the premises from which the cloud services are provided.	The EBA wishes to clarify that access to business premises (head offices and operations centres), which needs to be contractually ensured, should include access to data centres. The current wording, which refers to business premises (head offices and operations centres), is deemed to be sufficiently comprehensive. The EBA welcomes the suggestion and has amended the wording to clarify that access	Paragraph 10(b) has been amended to clarify that the audit rights should be related to the outsourced services.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		should be provided to the business premises, including the full range of devices, systems, networks and data, that are actually used for providing the services outsourced.	
4.3 Access and audit rights for competent authorities – Paragraph 10 – Written agreement	One respondent pointed out that the vast majority of agreements for cloud services are concluded online via electronic acceptance of standardised terms and conditions. The respondent proposed explicitly referring to electronically concluded agreements in the recommendations.	The EBA welcomes the comment and wishes to clarify that the term 'written agreement' is understood to cover agreements that are in electronic format.	No changes made.
4.3 Access and audit rights for competent authorities – Paragraph 11 – Contractual arrangements should not impede competent authorities in carrying out their supervisory functions and objectives	A few respondents requested that a standard contractual clause be provided with regard to the requirement for the contractual arrangements not to impede competent authorities in carrying out their supervisory functions and objectives.	The EBA welcomes the comment but wishes to allow sufficient flexibility for institutions to negotiate such contractual clauses in view of their specific requirements.	No changes made.
4.3 Access and audit rights for competent authorities – Paragraph 12 – Exercise of right to audit by competent authorities	A few respondents proposed specifying that competent authorities should exercise their rights of access and audit following the risk-based and proportionate approach proposed for institutions. Another respondent suggested explicitly linking the rights of access and audit for competent authorities to material outsourcing.	The EBA agrees that competent authorities need to exercise their rights of access and audit in a risk-based and proportionate manner. The EBA wishes to clarify that the rights of access and audit for competent authorities are not limited to material cloud outsourcing.	No changes made.
4.3 Access and audit rights for competent authorities – Paragraph 12 – Access to	One respondent emphasised the risks to security and data privacy if encryption methods and associated keys are provided to potentially	The EBA wishes to clarify that competent authorities would have access to the data through the outsourcing institution.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
encryption keys for competent authorities	multiple competent authorities without appropriate controls and protocols. Where access to underlying data is provided to competent authorities, for the performance of their supervisory duties, access to keys and encryption should be restricted, if not discouraged.	Therefore, competent authorities would not need access to encryption methods and associated keys.	
4.4 In particular for the right of access			
4.4 Right of access – Paragraph 14(a) – Notification of a planned onsite visit in a reasonable time period	A few respondents suggested clarifying what would be a 'reasonable time period' for the advance notification of a planned onsite visit to a cloud service provider. It was also suggested that information on both the scope of the visit and the participants be included in the advance notification of an onsite visit, to allow the cloud service provider to make the appropriate arrangements.	The recommendations intend to provide some flexibility with regard to the notification of onsite visits to cloud service providers, but it is explicitly mentioned that the timeframe should be reasonable.	No changes made.
4.4 Right of access – Paragraph 14	A few respondents proposed specifically adding that the exercise of the right of access for competent authorities should not create a risk for another client's environment or for the cloud service provider's business and operations. One respondent proposed inserting an additional specification that, in exercising the right to audit, outsourcing institutions and competent authorities should first pursue alternative ways to provide a similar level of assurance (third-party certification/audit reports) and exercise the right of	The EBA welcomes the comment and agrees that the exercise of the right of access by competent authorities should not create a risk for another client's environment or for the cloud service provider's business operations. The EBA wishes to clarify that flexibility in exercising the rights of access and audit both for institutions and for competent authorities needs to be maintained; therefore, any form of fixed hierarchy in the way the rights of	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	access only if these alternatives do not provide an adequate level of assurance.	access and audit should be exercised should be avoided.	
4.4 Right of access – Paragraph 14	One respondent argued that the focus of access rights should be on logical access to the institution's data stored or processed by the cloud service provider, and not on physical access to the premises of the provider.	The EBA wishes to clarify that for competent authorities and outsourcing institutions both physical and logical access need to be contractually agreed with the cloud service provider.	No changes made.
4.5 Security of data and systems			
4.5 Security of data and systems – Paragraph 15 – References to legal requirements	A few respondents suggested that the recommendations should refer to specific regulations (e.g. obligations resulting from the GDPR, the Directive on Security of Network and Information Systems (NIS) or the Payment Services Directive (PSD2)) and avoid any overlaps.	Specific references to other regulations are not included in the recommendations, since in any case it is not possible to refer to all existing national legislation on the security of data and systems, and the intention is to keep the recommendations future-proof. The requirements with regard to the security of data and systems included in the recommendations are specifically linked to the outsourcing context and should not duplicate any other regulations in that respect.	No changes made.
4.5 Security of data and systems – Paragraph 15 – Protection of information	A few respondents indicated that different types of cloud services function differently in terms of the level of involvement of cloud service providers in the processing and securitisation of data, depending on which service model is used.	The EBA would like to emphasize that the risk-based approach should enable the outsourcing institution to exercise its responsibility to determine the adequate level of safety and define the necessary security measures, taking into account the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		specific outsourcing context and only then will engage with the cloud service provider.	
4.5 Security of data and systems – Paragraph 16(a) and (b)	One respondent requested further clarification of whether the security classification and selection process in paragraph 16 should be seen as a requirement for material services only or whether it also applies to non-material cloud services.	The EBA wishes to clarify that all the provisions in the recommendations, including regarding the security classification and selection process in paragraph 16, apply to both material and non-material cloud outsourcing. The only exception is the duty to inform the competent authority under paragraphs 2 and 3, which applies only to material cloud outsourcing.	No changes made.
4.5 Security of data and systems – Paragraph 16(c) definition of appropriate level of protection of data confidentiality, continuity of activities outsourced	A few respondents pointed out that, while encryption is a powerful tool, not all forms of encryption are feasible in all cloud contexts. Furthermore, encryption technologies may evolve and become outdated in the future.	The EBA welcomes the comment and has amended the wording of paragraph 16 to clarify that security measures, such as the use of encryption technologies, should be considered by the outsourcing institution where necessary.	Paragraph 16(c) has been amended to clarify that the example of encryption is not limiting.
4.5 Security of data and systems – Paragraph 16(c)	A few respondents requested the inclusion of detailed guidance on what protection measures should be implemented.	The EBA would like to emphasize that the risk-based approach and the data classification should enable the outsourcing institution to determine the appropriate level of safety and define the necessary security measures, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.5 Security of data and systems – Paragraph 17 – Responsibility of cloud service providers	Several respondents indicated that the current formulation of paragraph 17 could give the impression that cloud service providers are responsible for all the requirements in paragraph 16(c) (whereas it is the outsourcing institution that is responsible for 'defining and deciding on an appropriate level of protection in terms of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems').	The EBA welcomes the comment and has amended the wording to avoid giving the impression that the cloud service provider is responsible for all the tasks in paragraph 16(c).	Paragraph 17 has been amended to clarify that not all the requirements in paragraph 16(c) are the responsibility of the cloud service provider.
4.5 Security of data and systems – Paragraph 18 – Monitoring of the performance of activities and security measures	One respondent requested examples of how outsourcing institutions should monitor the performance of activities and security measures.	The EBA wishes to clarify that flexibility is provided to the outsourcing institutions with regard to defining the performance of the activities and the security measures, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	No changes made.
4.6 Location of data and data processing			
4.6 Location of data and data processing – Paragraph 19	One respondent proposed including a more specific reference to the CEBS guidelines in paragraph 19.	The EBA welcomes the comment and has amended the text accordingly.	Paragraph 19 has been amended to include a more specific reference to the CEBS guidelines.
4.6 Location of data and data processing – Paragraph 19	A few respondents considered that the requirement for institutions to take 'special care' when entering into and managing outsourcing	The EBA wishes to clarify that paragraph 19 refers to a requirement included in the CEBS	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	agreements outside the EEA may not be enough to properly enforce and supervise the current EU regulatory framework in relation to contractual arrangements for outsourcing to cloud service providers. The respondents suggested adding the requirement that outsourced data should stay in the EEA and that the localisation and processing of data outside the EEA is allowed only in cases in which the data are actually exchanged between data centres inside and outside the EEA. Another respondent proposed removing the requirement for outsourcing institutions to take 'special care when transferring data outside the EEA' because it creates ambiguity about how outsourcing institutions can address data location risks.	guidelines, and therefore cannot be amended in these recommendations.	
4.6 Location of data and data processing – Paragraph 20 – Additional references to data protection rules	A few respondents recommended that the EBA confirm that the recommendations do not impose requirements distinct from or additional to those set out in existing data protection regulation. One respondent suggested adding a reference to data protection rules to the requirements around the location of data and data processing. Another respondent suggested removing the reference to laws on data protection, since they are already covered by current laws and the GDPR.	The recommendations do not provide any detailed requirements on the location of data and data processing in addition to existing data protection regulation. Rather, institutions are requested to adopt a risk-based approach in considering data and data processing locations, taking into account the legal framework in force. The aspect of data protection is highlighted in the recommendations in view of its potential impact on prudential risks; the provisions are specifically linked to the outsourcing context	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		and should not duplicate any other regulations.	
4.6 Location of data and data processing – Paragraph 20 – Changes in data location	One respondent pointed out that most cloud service providers require the contractual right to change a data processing location without the institution's consent. However, moving a data location can cause institutions to breach data protection rules and regulations that restrict the offshoring of data. The respondent asked the EBA to provide further guidance on this issue, in particular regarding the notification of such changes and the right of the outsourcing institution to terminate the contract in such a case.	The EBA wishes to clarify that the example given would fall under the contractual agreement between the outsourcing institution and the cloud service provider.	No changes made.
4.6 Location of data and data processing – Paragraph 20	One respondent recommends that the guidance emphasise that cloud service providers should ensure, without unnecessary extra costs and limitations, the effective migration of data to another cloud service provider on request. Moreover, cloud service providers should ensure that regulated entities can meet regulatory compliance requirements, such as requirements on data subject rights, as set forth in the GDPR, in accordance with which data subjects can exercise their rights with respect to data controllers.	The arrangements referred to would fall under the contractual agreement between the outsourcing institution and the cloud service provider.	No changes made.
4.7 Chain outsourcing			

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.7 Chain outsourcing – Responsibility of outsourcing institutions	Several respondents pointed out that, as outsourcing institutions have less power when outsourcing to cloud service providers, they should have fewer duties as well. Furthermore, the cloud service provider should remain responsible for the activities it further outsources, just as the outsourcing institution remains responsible for the activities it outsources. This should be ensured through the contractual arrangement.	The EBA acknowledges that there might be differences in bargaining power. The requirements on chain outsourcing are intended to avoid any adverse effects on the service provided by cloud service providers as a result of chain outsourcing. In this respect, it is expected that these expectations, in the form of EU-wide recommendations, can assist institutions in their negotiations with cloud service providers.	No changes made.
4.7 Chain outsourcing – Responsibility of subcontractors	Several respondents suggested that the requirement for subcontractors to fully comply with the obligations existing between the outsourcing institution and the cloud service provider is formulated too broadly. Respondents pointed out that subcontractors would often only perform a limited subset of the services provided by the cloud service provider to the outsourcing institution and that they therefore should have more limited responsibility. One respondent pointed out that ICT supply chains continue to expand, making secure and reliable chain management of sub(sub)contractors very difficult and expensive. It was also noted that it is important that a contract with a subcontractor should conform with, or at least not contradict, the requirements of the agreements between the cloud service provider and the outsourcing institution. In view of the	The EBA welcomes the comment and wishes to clarify that the wording in paragraph 21 is a provision from the CEBS guidelines and can therefore not be amended in the context of these recommendations. The outsourcing institution should give its consent to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider. Similar to outsourcing institutions, cloud service providers cannot outsource the responsibility.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	more limited subset of tasks of the subcontractor, it is not feasible for the service agreement between the cloud service provider and the subcontractor to fully reflect the agreement between the outsourcing institution and the cloud service provider.		
4.7 Chain outsourcing – Scope	A number of respondents asked for clarification of which activities are within the scope of the requirements on subcontracting. A few respondents proposed limiting the requirements on chain outsourcing to material cloud outsourcing that concerns services whereby the subcontractor has access to the outsourcing institution's data. Other respondents proposed distinguishing between subcontracting and auxiliary services or limiting the requirements to those subcontracted functions that are relevant for the provision of a regulated financial service.	The EBA wishes to clarify that the activities in the scope of the requirements on subcontracting are broader than just the data and go beyond material or regulated services. Furthermore, continuity of services is important.	No changes made.
4.7 Chain outsourcing – Localisation of data	One respondent suggested that special consideration be given to the localisation of the data in cases of chain outsourcing. The respondent urged the competent authorities to take a rather strict approach in relation to cloud service providers outsourcing cloud services to providers that place data outside the EEA.	The EBA wishes to clarify that existing laws and regulations, albeit not explicitly referred to in the recommendations, remain applicable. Special care should be taken with regard to outsourcing agreements outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authorities, as indicated in paragraph 19.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.7 Chain outsourcing – Paragraph 21 – Responsibility of the outsourcing institution	A few respondents indicated that the responsibility of the outsourcing institution to ensure that the subcontractor fulfils its contractual obligations to the contracting cloud service provider is formulated too broadly. The respondents argued that the diligence, risk assessments, controls and checks should be conducted by the cloud service provider to ensure that all subcontractors meet the security warranties and comply with the provisions mentioned in the contract.	The EBA wishes to clarify that, while the outsourcing agreement should indicate that the cloud service provider retains full responsibility for and oversight of the services that are subcontracted, the outsourcing institution remains responsible for monitoring the overall service it receives, regardless of whether it is provided by the cloud service provider or by a subcontractor further down the chain.	No changes made.
4.7 Chain outsourcing – Access/audit rights to subcontractors	A few respondents asked for clarification of whether the outsourcing institution and/or the competent authority should retain access and audit rights at the level of the subcontractor. One respondent pointed out that, in practice, contracts often limit institutions' audit rights to subcontractors of cloud service providers. Some cloud service providers limit audit rights to sub-processors that process personal data on behalf of the institution only. Alternatively, it was suggested that allowing the possibility of auditing subcontractors if they contribute materially to the service performed be considered.	The EBA wishes to clarify that the access and audit rights at the level of the subcontractor should form part of the contractual arrangement between the outsourcing institution and the cloud service provider. The outsourcing institution should make sure that those rights can also be exercised at the level of the subcontractor.	No changes made.
4.7 Chain outsourcing – Paragraph 22 – Outsourcing agreement – Exclusion of activities from potential subcontracting	A few respondents pointed out that, because of the high degree of standardisation of services, cloud service providers may not be able to	The EBA wishes to clarify that the recommendations allow individual institutions to decide which of the activities they are outsourcing to the cloud service	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	contractually agree not to subcontract specific types of activities for individual clients. It was also suggested that areas that should be included in or excluded from potential subcontracting be specified.	provider should be excluded from subcontracting in view of their particular requirements and the cloud service arrangement they have with their cloud service provider. It is expected that these expectations, in the form of EU-wide recommendations, can assist institutions in their negotiations with cloud service providers.	
4.7 Chain outsourcing – Paragraph 23 – Cloud service providers to inform institutions about significant changes in subcontracting	Several respondents proposed including a definition or examples of what would be considered a 'significant change' to the subcontractors or subcontracted services, as well as a timeframe for notifications by cloud service providers.	The EBA wishes to clarify that the recommendations allow individual institutions to decide what would constitute significant changes in subcontracting and what would be the most appropriate timeframe for the notifications in view of their particular requirements, their risk assessments and the cloud service arrangement they have with their cloud service provider.	No changes made.
4.7 Chain outsourcing – Paragraph 23 – Information on planned changes in subcontracting	A few respondents asked the EBA to clarify that there is no requirement for active consent from the outsourcing institution to chain outsourcing by the cloud service provider.	The EBA wishes to clarify that, although cloud service providers need to inform the outsourcing institution of any planned significant changes in subcontracting, no active consent is needed from the outsourcing institution to those changes. The outsourcing institution should have the right to terminate the contract in case these changes will have an adverse effect on the risk assessment of the agreed services.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.7 Chain outsourcing – Paragraph 23 – Information on planned changes in subcontracting	One respondent asked if the requirement for notification by the cloud service provider of planned changes in subcontracting without the requirement for pre-approval of these changes by the outsourcing institution supersedes national regulations that are more restrictive on that topic (and require pre-notification).	The EBA would like to clarify that the provisions of national legislation would prevail over those of the recommendations, which are not a legally binding instrument. However, through the 'comply or explain' principle, competent authorities are expected to implement the recommendations within the local regulatory and legislative framework.	No changes made.
4.7 Chain outsourcing – Paragraph 23 – Notification of significant changes to subcontracted services	One respondent suggested that the word 'proposed', with regard to significant changes to subcontractors or subcontracted services, implies that the institution has a right to agree or disagree with a proposed change and suggested rewording this.	The EBA welcomes the comment and agrees that the use of the word 'proposed' could give the impression that changes to subcontracting are subject to approval. The wording has been amended accordingly.	Paragraph 23 has been amended to make reference to 'planned' changes to subcontracting.
4.7 Chain outsourcing – Paragraph 23 – Risk assessment	A few respondents noted that it is not clear if it is optional or mandatory for the outsourcing institution to perform a risk assessment when it is informed by the cloud service provider of a planned significant change in subcontracting.	The EBA wishes to clarify that an outsourcing institution would be required to perform a risk assessment if its cloud service provider informed it about a planned significant change in subcontracting. The scope and depth of this assessment may vary.	No changes made.
4.7 Chain outsourcing – Paragraph 24 – Right to terminate the contract	One respondent suggested that the right to terminate the contract should be explicitly called out within the contract in writing. The contract must clearly define the terms under which a party can terminate and under what conditions. Another respondent asked for the right of termination to be limited to quantifiable and material adverse risks.	The existence of an early termination clause in the contract is already implied in the text. The outsourcing institution should be able to exit the outsourcing agreement if the change in subcontracting affects the risk exposure to a degree that is not acceptable to the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	It was also pointed out that any termination of the contract by the outsourcing institution would usually require a contractual default.	institution (even if the actual service levels are not yet affected).	
4.7 Chain outsourcing – Paragraph 25 – Review and monitoring of overall service performance	A few respondents suggested that the outsourcing institution should be able to rely on the outsourcing service provider to perform any due diligence requirements around subcontracting requirements. One respondent proposed that the EBA clarify whether the institution needs to directly monitor and review the performance of each subcontractor or whether the requirement is limited to directly monitoring the service provider. The respondent also proposed specifying how many layers of subcontractors are allowed.	The EBA wishes to clarify that, although the cloud service provider is responsible for providing the service agreed with the outsourcing institution, the outsourcing institution should have oversight of the overall service provided regardless of whether it is provided through subcontractors. This does not imply a requirement for the outsourcing institution to monitor and review the individual performance of each subcontractor. The recommendations do not specify any limit to the number of layers of subcontractors.	No changes made.
4.8 Contingency plans and exit strategies			
4.8 Contingency plans and exit strategies – Exit strategy and exit plan	One respondent asked for clarification of whether the requirements on exit strategies relate also to exit plans.	The EBA wishes to clarify that the exit plan is a more operational plan to implement the overall exit strategy.	No changes made.
4.8 Contingency plans and exit strategies – General remarks	One respondent requested clarification of whether the requirements on contingency plans and exit strategies are applicable only to material cloud outsourcing or if they apply also to non-material cloud outsourcing.	The EBA clarifies that all the provisions in the recommendations, including the requirement to develop contingency plans and exit strategies, apply to both material and non-material cloud outsourcing. The only exception is the duty to inform the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	A few respondents requested more guidance on the level of detail with respect to the continuity arrangements (e.g. do institutions need to have contracts with backup service providers in place?).	competent authority under paragraphs 2 and 3, which is required only for material cloud outsourcing. The recommendations allow sufficient flexibility for outsourcing institutions to determine the appropriate continuity arrangements, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context. Any backup solutions should be practical and sufficiently tested where appropriate.	
4.8 Contingency plans and exit strategies – General remarks	One respondent requested clarification of how the requirement for institutions to develop contingency plans and exit strategies relates to the requirement for institutions to keep in a register information on the assessment of the cloud service provider's substitutability.	The assessment of the substitutability of cloud service providers is aimed at identifying the ease and speed with which the outsourcing institution can move its activities from the cloud outsourcing provider to an alternative provider. The development of contingency plans and exit strategies is intended to prepare the institution for the actual execution of the transfer of its activities to an alternative provider. Subsequent to the abovementioned assessment, the outsourcing institution needs to include the following information in the register on cloud outsourcing activities: (i) if the cloud service provider's substitutability is considered easy, difficult	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		or impossible and (ii) which alternative service has been identified.	
4.8 Contingency plans and exit strategies – Paragraph 27(a) – Testing of exit strategies	Several respondents indicated that the testing of exit strategies is not realistic. The respondents argued that any exit from a cloud service involves careful planning, data capacity network analysis, setting up migration structures and governance models, increased staffing, purchasing IT systems, temporary upgrades to network bandwidth, etc. Therefore, it is not realistic to fully test the exit strategy. Other respondents proposed including detailed guidance on the testing of exit plans.	The EBA wishes to clarify that the testing is to be performed only 'where appropriate' and can be done in the form that the outsourcing institution deems most appropriate, whether it be a desktop exercise, live testing or some other form.	No changes made.
4.8 Contingency plans and exit strategies – Paragraph 27(b) – Destruction of data	One respondent indicated that assured data destruction is a highly relevant topic when exiting cloud providers. Although the means to achieve safe data destruction may vary considerably across cloud services, the requirement to both destroy data securely and demonstrate evidence of this is a key security principle and should be explicitly stated.	The EBA welcomes the comment about the relevance of assured data destruction and agrees with the importance of the safe destruction of data from live, backup and archive environments, and other copies, as well as the related key management. This should form part of the exit plan.	No changes made.
4.8 Contingency plans and exit strategies – Paragraph 27 – Alternative solutions	One respondent suggested making allowances for situations where the solution is innovative and is provided by a limited number of service providers, so that migration to another provider is not feasible.	The EBA wishes to clarify that outsourcing institutions should make sure that the alternative solution they identify is practical for them. Furthermore, where the solution is innovative and provided by a limited number	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		of service providers, an alternative solution should be put in place.	
4.8 Contingency plans and exit strategies – Paragraph 27(c) – Additional details	One respondent stated that the continuity plan and the exit solution should be the responsibility of the cloud service provider and that this should be reflected in the contractual arrangement between the outsourcing institution and the cloud service provider.	The EBA wishes to clarify that the outsourcing institution remains responsible for developing contingency and exit plans and ensuring the outsourcing agreement includes an obligation on the cloud service provider to sufficiently support the orderly transfer of the activity in the event of an exit.	No changes made.
4.8 Contingency plans and exit strategies – Paragraph 27(c) – Transfer of data	Several respondents pointed out that an unqualified obligation on the cloud service provider to transfer the activity to another service provider or to the outsourcing institution may not work in all cloud service models. Although the cloud service provider makes tools and functionality available to the customer, the customer operates these tools and is in control of the upload and retrieval of its data.	The EBA welcomes the comment and agrees that the outsourcing institution remains responsible for the transfer of the data and that the cloud service provider should provide adequate support for an orderly transfer in the event of an exit.	Paragraph 27(c) has been amended to indicate that the outsourcing agreement should include an obligation on the cloud service provider to sufficiently support the outsourcing institution in the orderly transfer of the activity.
4.8 Contingency plans and exit strategies – Paragraph 28(d) – Criteria for successful exit strategy	A few respondents requested the removal of the requirement for outsourcing institutions to define criteria for a successful exit strategy, as these would be redundant and overly burdensome.	The EBA wishes to clarify that, although the transition is successful if the retracted business processes operate successfully in the new environment, it still makes sense to	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		set out criteria for the transition, for example in terms of timing.	
4.8 Contingency plans and exit strategies – Paragraph 29 – Triggering of the exit plan	A few respondents pointed out that a breach of service monitoring thresholds should not trigger the exit plan immediately; rather, it should trigger a discussion and further investigation or a remediation plan.	The EBA welcomes the comment and would like to explain that the triggering of the exit plan would not be immediate. It is still important that there are key risk indicators in place that can trigger an exit. The design and setting of such indicators is important and needs to sufficiently take into account actual impact.	No changes made.
Section 5.1 – Impact assessment	One respondent requested that Article 35 of the GDPR on data protection impact assessment should be taken into account in relation to the impact assessment and with regard to the cloud service provider's obligation to carry out a risk assessment, even in a general way, to enable financial/outsourcing institutions to understand and evaluate the risks of using a cloud service provider. The respondent also requested that the recommendations expressly refer to the NIS Directive; the respondent favours harmonisation of cybersecurity incident notifications to ensure a consistent approach, as well as allowing for a broad scope of incident reporting, including reporting of imminent threats. Another respondent asked for the EBA to clarify that no further notification obligations are imposed on financial institutions in respect of personal data	The EBA welcomes the suggestions and would like to clarify that existing laws and regulations, albeit not explicitly referred to in the recommendations, remain applicable. The requirements with regard to the security of data and systems included in the recommendations are specifically linked to the outsourcing context and should not duplicate any other regulations. The recommendations do not include specific requirements for reporting security incidents, since this topic is deemed to be more broadly applicable than to the context of cloud outsourcing and is also addressed in the existing regulatory and legislative framework.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	security breaches and security incidents governed by the GDPR and NIS directives.		
Section 5.1 – Impact assessment	Regarding the provision 'capacity of the regulated institution to re-enter the data or services' one respondent asked for further clarification of what this means in practice and what 're-enter' means.	The EBA would like to clarify that 'to re-enter the data or services' refers to the outsourcing institution re-insourcing activities or services that were previously outsourced.	No changes made.
Responses to questions in Consultation Paper EBA/CP/2017/06			
Question 2. **Are there any additional areas that should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?**			
Further harmonisation and collaboration across the industry	A number of respondents suggested further collaboration between the relevant stakeholders (institutions, cloud providers and regulators) to combine efforts on standards on reporting, audit and access rights, and exit plans. One respondent proposed harmonising cloud services requirements across all jurisdictions, or at least at EU level, so as to avoid divergence in approaches. Harmonisation could bring greater certainty to institutions and suppliers when designing and managing solutions and assist in compliance. It could also assist in the development and use of cloud services on a more cost-effective basis.	The EBA welcomes the comment and agrees that there is a need for a common approach to requirements in relation to cloud computing. These recommendations constitute a first step in this direction by providing common EU-wide guidance for both institutions and supervisors, and they are expected to be implemented by the EU competent authorities under the 'comply or explain' principle. The EBA intends to engage with the sector and provide further guidance to assist convergence in the implementation of the recommendations in the form of a formal Q&A process.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
References to other EU regulations and directives	A number of respondents requested the inclusion of additional references to key EU regulatory requirements (e.g. the NIS, GDPR and PSD2 directives) and technical standards bodies (e.g. ISO).	Although these recommendations are harmonised with the broader regulatory context, references to other regulatory products might not serve the objective of future-proofing these recommendations.	No changes made.
Minimum contractual arrangements between cloud service providers and institutions	A number of respondents commented on the differences in negotiating powers between outsourcing institutions and cloud service providers, and suggested setting core minimum contractual arrangements at EU level between cloud service providers and their users. Similarly, it was suggested that competent authorities should engage directly with cloud service providers on financial services outsourcing requirements to achieve a common understanding of industry standards and ease compliance efforts. Another respondent proposed developing an assessment guide for the security of cloud service providers in financial services, as this could help outsourcing institutions and supervisors to assess compliance with the recommendations in the course of their auditing duties.	The EBA wishes to clarify that the responsibility and freedom to determine the contractual arrangements in outsourcing agreements should remain with institutions. These EU-wide recommendations are expected to assist institutions in their negotiations with cloud service providers. The EBA welcomes the suggestion and notes that the security of cloud service providers should be a key priority for outsourcing institutions. This could be a potential area for future work after the implementation of these recommendations.	No changes made.
Voluntary certification of cloud service providers/cloud solution providers	Several respondents proposed the introduction of a voluntary certification for cloud service providers, whereby a cloud service provider could request a prior review by the competent authorities. A positive outcome could facilitate a 'fast-track' outsourcing notification procedure. This could also	The EBA welcomes initiatives for voluntary certification of cloud service providers but wishes to safeguard respect for the freedom of contractual choice and the independence of both institutions and competent authorities. Furthermore, voluntary	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	help outsourcing institutions where competent authorities identify cloud service providers that do not have the capacity to allow institutions to comply with the applicable requirements. An alternative could be for the competent authorities to accept certifications similar to those mentioned in the NIS Directive.	certifications should not be perceived as a waiver from competent authorities.	
Additional areas to be explored	Other areas that could be explored, as suggested by one respondent, include key management and encryption, and areas where cloud services would require special consideration, such as incident management, change management, disaster recovery and business continuity management.	The EBA welcomes the proposals for additional areas to be explored and points out that some of the proposed areas have already been covered in previous work, such as in the EBA ICT risk assessment guidelines.	No changes made.
Nature of shared responsibility model	One respondent proposed describing the nature of the shared responsibilities of cloud service providers and outsourcing institutions to allow clear lines of responsibility.	In view of the different types of cloud environments, the EBA intends to allow institutions sufficient flexibility in this respect, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.	No changes made.
Concentration risk and cloud service providers' bargaining power	A few respondents suggested direct applicability of regulatory minimum requirements/safeguards and supervision of large cloud service providers or a similar mechanism as a way to reduce concentration risk at industry level where large cloud service providers can become a single point of failure when many institutions rely on them. This could also balance the bargaining power of cloud	The EBA wishes to clarify that, as cloud service providers are not within the scope of these recommendations, it is the responsibility of the institutions to discuss and agree the exact contractual arrangements in their outsourcing agreements with cloud service providers.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	service providers when it comes to negotiating contractual terms. Similarly, a respondent suggested placing less emphasis on the resilience of a single cloud service provider and encouraging the deployment of multiple cloud service providers. The combination of multi-sourcing of cloud service providers with resilient architectures created by institutions would be beneficial for systemically important services, reduce concentration risk and reduce disruption when exiting a cloud service provider. Another respondent pointed out that it would be critical for institutions to have more than one cloud service provider and have critical applications able to run on multiple clouds at the same time. A few respondents noted that no description is currently included in the recommendations on how systemic risks should be handled.	While concentration risk could be present at both micro and macro levels, these recommendations facilitate the collection of sufficient information by competent authorities for monitoring concentration risk at industry level, where macroprudential authorities should handle any systemic risks raised.	
Service model coverage	A respondent noted that the recommendations primarily focus on IaaS and not on the other cloud-based services. For example, additional issues related to SaaS should be addressed, such as updates to and maintenance of applications, and service level issues. Such guidance could help institutions to better identify and contract for services that meets their requirements.	The EBA wishes to clarify that the recommendations apply to all cloud service models, as they are service-model agnostic, to keep the recommendations technology-neutral and future-proof.	No changes made.
Transitional implementation period	Some respondents proposed allowing a 24-month period to fully implement the recommendations. In particular, amendments to underlying outsourcing	As these recommendations will be applicable to any new cloud outsourcing agreements or revision of existing cloud outsourcing	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	agreements as well as to the implementation and maintenance of registers are expected to be time-consuming processes.	agreements, the application date is deemed to be sufficiently conservative.	
Further guidance on contractual terms with cloud service providers	A few respondents proposed including guiding principles for contractual terms with cloud service providers covering the specific needs of the banking sector with the aim of also accommodating GDPR requirements to guarantee legal certainty and facilitate the adoption of the cloud by financial institutions. It was also suggested that reference should be made to standards and regulations that should be captured in outsourcing contracts and that a risk management guide for financial cloud-based services could be developed that could serve as a common basis for financial institutions' contractual provisions in terms of the security of financial cloud infrastructures.	The EBA wants to clarify that the main objective of these recommendations is to specify a set of principles that complement and update the CEBS guidelines and which competent authorities can apply within their regulatory and supervisory frameworks on the cloud outsourcing process and the associated risks. Related guiding principles for contractual terms are already included in the recommendations.	No changes made.
Data protection	In relation to the transfer of personal data and data localisation, one respondent noted that competent authorities should align with the decisions of the data protection authorities if they have authorised the transfer of data to certain countries complying with the GDPR. Moreover, the competent authorities should abide by the GDPR and the decisions of the data protection authorities if they have granted permission to use a cloud service complying with all security and privacy measures.	The recommendations do not provide any detailed requirements on the location of data and data processing in addition to the existing data protection regulation. Rather, institutions are requested to adopt a risk-based approach in considering data and data processing locations, taking into account the legal framework in force. The importance of data protection is emphasised in the recommendations in view of its potential impact on prudential risks; the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	One respondent proposed that the recommendations should focused more on data and assist institutions in understanding the challenges associated with data security, data classification, data retention and data deletion.	requirements in this regard are specifically linked to the outsourcing context and should not duplicate any other regulations.	
Risk prioritisation on cloud outsourcing strategy	One respondent proposed that the recommendations should mention how risks related to cloud outsourcing strategy should be prioritised, so as to provide institutions with a framework on or approach to allocating their budgets and planning the necessary changes and improvements.	The EBA wishes to clarify that these recommendations should be seen as principle-based, providing guidance that can be applied in different practical situations and that can be adapted to the changing business environment. Moreover, the responsibility to prioritise risks lies with the institutions and these priorities should be clearly set out in the relevant risk assessments.	No changes made.
Security notification regime	One respondent recommended clarifying the extent to which institutions must notify regulators when adverse technology events occur and how these notification procedures relate to those required under data protection laws and decisions taken at regional level in respect of the NIS Directive to the banking sector. The purpose would be to avoid inconsistencies arising in the approaches that EU Member States and the competent authorities take to obligations under the NIS Directive and those under the financial regulatory framework.	The proposed clarification regarding security notifications does not fall within the scope of these recommendations. The recommendations do not include specific requirements for reporting security incidents, as this topic is deemed to be more broadly applicable than to the context of cloud outsourcing and is also addressed in the existing regulatory and legislative framework.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Inclusion of provisions on mobile cloud computing	One respondent suggested that it would be beneficial to add specific provisions on mobile cloud computing, as mobile cloud computing has a longer processing chain involving more stakeholders, which entails additional vulnerabilities and more investment in security to be shared/coordinated to ensure safe use of the cloud.	The EBA welcomes the comment about the specificities of mobile cloud computing and wishes to clarify that the recommendations would also apply to this specific form of cloud outsourcing in a proportionate manner.	No changes made.