EBA/CP/2017/06

17/05/2017

Consultation paper

Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010[1]

[1] 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.

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 18.08.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive summary

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

Whereas general outsourcing guidelines have been in place since 2006 under the form of the CEBS guidelines on outsourcing ("CEBS guidelines")[2], the outsourcing framework is constantly evolving. Over recent years, there is an increasing interest of institutions for using the services of cloud service providers. Where the CEBS guidelines remain applicable for 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 all institutions as set out in the CEBS guidelines. The principle of proportionality should apply 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 the cloud outsourcing determines whether institutions are required to adequately inform their competent authority about the cloud outsourcing. Specific guidance is included on the process and content for institutions to inform their competent authorities about material cloud outsourcing.

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

Due to 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 needed.

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 in the context of cloud outsourcing.

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

3. Background and rationale

1. In accordance with Article 16 of Regulation (EU) No 1093/2010[3] ("the EBA regulation"), the EBA shall issue guidelines and recommendations addressed to competent authorities, 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 are outsourcing to cloud service providers. To that end these recommendations add on the guidance provided in the CEBS guidelines.

3. The EBA identified the need for developing specific guidance for outsourcing to cloud service providers following interactions with several stakeholders. It appeared 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 the cloud services. There are some differences in the national regulatory and supervisory frameworks for cloud outsourcing for example with regards to the information obligations applying to institutions towards competent authorities.

4. Compared to more traditional forms of outsourcing offering tailor made solutions for clients, cloud outsourcing services show a much higher level of standardization which allows the services to be provided to a larger number of different customers, in a much more automated manner on a larger scale. Whereas cloud services can offer a number of advantages such as economies of scale, flexibility, operational efficiencies, and cost-effectiveness, it also raises 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 where large suppliers of cloud services can become a single point of failure when many institutions rely on them.

5. The aim of these recommendations is to:

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

6. The recommendations focus on the well-known and important areas for further supervisory alignment and/or clarification as highlighted by stakeholders.

[3] 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.

7. An area in which different practices were observed amongst Member States is on the duty for outsourcing institutions to adequately inform their competent authority about material (cloud) outsourcing. Therefore specific guidance is included on the process and content for institutions to inform their competent authorities about material cloud outsourcing.

8. The right to audit is a key right laid down in the principles of the CEBS guidelines which is restated in these recommendations. Further guidance is provided on the way in which institutions can exercise this right to audit in a risk based and proportionate manner accommodating concerns with regards to organizational burdens both for the outsourcing institution and the service provider, and with regards to practical, security or 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 are sharing access to a set of physical and virtual resources although their data are isolated from one another).

9. The CEBS guidelines have already provided guidance on issues like information confidentiality and system availability. These recommendations elaborate further on the need for integrity and traceability, establishing an approach as to how security should be assessed in case institutions are outsourcing activities to cloud service providers. Against this background, these recommendations aim to address the 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 aiming at keeping record of technical and business operations are also key to detect malicious attempts to the security of data and systems. According to the proportionality principle, security expectations should take into account the need for protection of the data and systems.

11. As cloud service providers often operate a geographically dispersed computing infrastructure that entails a regional and/or global distribution of data storage and processing, the recommendations provide specific requirements for data and data processing locations in the context of cloud outsourcing. Notwithstanding this guidance, in any case Union and national law in this respect applies, in particular in 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 that regard, cloud outsourcing is more dynamic in nature than traditional outsourcing setups. To that end, there is a need for enhancing certainty as to the conditions under which subcontracting can take place in the case of cloud outsourcing. Against this background, the recommendations provide that, subcontracting requires ex ante notification to the outsourcing institutions, 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 the planned changes of subcontracted services will have an adverse effect on the risk assessment of the outsourced services.

13. The recommendations are not exhaustive, nor should they be read in isolation from the CEBS guidelines.

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

EBA/REC/2017/XX

DD Month YYYY

4. Recommendations (DRAFT)

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[4]. 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 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 whom 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 EBA.

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

[4] 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 the 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 credit institutions and investment firms as referred to in Article 4(1) of Regulation No 1093/2010.

Definitions

3. Unless otherwise specified, terms used and defined in Directive 2013/36/EU[5] 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	cloud computing 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 which is a composition of two or more distinct cloud infrastructures.

[5] 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.

Infrastructure as a Service (IaaS)	cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.
Platform as a Service (PaaS)	cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.
Software as a Service (SaaS)	cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3. Implementation

Date of application

5. These guidelines apply from dd.mm.yyyy

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 the activities' materiality on the basis of CEBS guidelines and, in particular as regards outsourcing to cloud service providers, taking into account all of the following:

    (a) the criticality and inherent risk profile of activities to be outsourced i.e. 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 any disruption of the activity might have on their 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 being 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:

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

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 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 a termination by either party or disruption of provision of the services by the cloud service provider;
(c) whether the outsourcing institution keeps the skills and resources necessary to adequately monitor the outsourced activities.

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

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

(a) those information referred to in paragraph 2 a) to g) if not yet provided;
(b) type of outsourcing (IaaS, PaaS, SaaS, public/private/hybrid/community);
(c) parties receiving cloud services under the outsourcing agreement;
(d) approval for outsourcing by the management body or the committee designated by it;
(e) name of the main subcontractor if applicable;
(f) country where the cloud service provider / main subcontractor is registered;
(g) whether the outsourcing has been assessed as material (yes /no);
(h) date of institution's last materiality assessment of the outsourced activities;
(i) cloud service provider / significant subcontractor supports business operations that are time critical (yes/ no);
(j) assessment of the cloud service provider's substitutability as easy, difficult or impossible;
(k) identification of an alternate service provider, where possible;
(l) date of the last due diligence on 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, 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 (right of audit).

7. The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. When 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 upon.

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

   (a) Pooled audits performed jointly with other clients of the same cloud service provider in order to use audit resources more efficiently and to decrease the organizational burden both to clients and to 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 centers, etc.) which are relevant to the institution and the controls identified as key by the outsourcing institution.
      ii. The outsourcing institution thoroughly assesses the content of the certifications or audit reports continuously, 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. rotation of the certifying or auditing company, qualification, expertise, re-performance/verification of the evidence in the underlying audit file).
      iv. The certifications and audits are done against widely recognized standards and contain a test of 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 which 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 present a high level of technical complexity, the outsourcing institution should verify that the staff performing the audit – being its internal auditors or 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 audit and/or assessment 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 centers), including in 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 of the outsourcing institution's data (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. Competent authorities should exercise their rights of access and audit, only to perform their supervisory tasks and ensure financial stability. Information, which competent authorities obtain from the exercise of those rights, should be subject to the professional secrecy and confidentiality requirements referred to in Article 53seq. of Directive 2013/36/EU ("CRD IV"). Competent authorities should refrain from entering into any kind of contractual agreements or declarations that would prevent them from abiding to 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 or impose measures directly on the outsourcing institution.

4.4 In particular for the right of access

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

    (a) The person 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 on site 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 co-operate 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), 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) institutions should implement arrangements to ensure the continuity of the services provided by the outsourcing service provider. Building on guidelines 8 (2) (b) and 9 of the CEBS guidelines, the respective needs of the outsourcing institutions with respect to quality and performance should feed into a written outsourcing contract 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, institutions 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 its activities, processes and related data and systems which are being considered to be outsourced to a cloud computing solution;

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

17. Subsequently, institutions should ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligations under paragraph 16 (c).

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 and should promptly take any corrective measures thereto.

4.6 Location of data and data processing

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

20. The outsourcing institution should adopt a risk-based approach in considering data and data processing location considerations when outsourcing to a cloud environment. The assessment should address the potential risk impacts, legal risks and compliance issues, and oversight limitations related to the countries where the outsourced services are or is likely to be provided and data is or is likely to be stored. The assessment should include considerations on the wider political and security stability of the jurisdictions; the laws in force in the jurisdictions in question (including laws on data protection); and the law enforcement provisions within the jurisdictions including insolvency law provisions in case of a cloud service provider failure. An 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 and oversight of those services that they have subcontracted.

23. The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution on any proposed significant changes to the subcontractors or the subcontracted services named in the initial agreement, which may 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 to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.

24. In the case that the cloud service provider plans changes of a subcontractor or subcontracted services which will 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) point e) and 8 (2) point d) of the CEBS guidelines, the outsourcing institution should plan and implement arrangements to maintain the continuity of their business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree. This policy should include contingency planning and a clearly defined exit strategy. Furthermore, the outsourcing contract should include a termination and exit management clause which 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 they are able to exit cloud outsourcing arrangements if needed without undue disruption to their provision of services, or adverse effects on their 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 be able 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 maintain business continuity during the transition phase.

(c) Ensure the outsourcing agreement includes an obligation on the cloud service provider to orderly transfer the activity and that of the subcontractors to another service provider or to the direct management of the outsourcing institution in case of the termination of the outsourcing agreement.

28. When developing exit strategies outsourcing institutions should consider the following:

(a) Develop key risk indicators that should identify unacceptable level of services.

(b) Perform a business impact analysis that is commensurate to the activities outsourced to identify what human and material resources would be required to implement the exit plans and how much time it will 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 their ongoing service monitoring and oversight of the services provided by their cloud service provider.

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

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

As per 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'. Such annex shall 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 annex presents the impact assessment with 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 for the 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, e.g. while there is demand for outsourcing, the institutions may decide not to opt for this option due to regulatory uncertainty. Furthermore, the lack of an effective regulatory framework is expected to have a higher 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 entire process that the current regulatory framework does not fully cover for the context of cloud sourcing. The absence of a more effective framework increases the risk profile of such events: the lack of specific guidance and a more detailed assessment for supervisors to assess outsourcing risk may lead to an incomplete risk assessment of an institution 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 for the

regulatory framework and supervisory assessment of outsourcing risks in EU institutions and therefore room for inconsistency in assessing outsourcing risk across jurisdictions leading to a lack of comparability of supervisory practices across EU which is of crucial importance given the cross-border nature of the cloud service. 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 of the member states have comprehensively transposed the CEBS guidelines: a survey carried out by the EBA (completed on 18 September 2015) indicates that of the 24 national frameworks[6], 53% totally transposed, 38% partially transposed, 8% did not transpose the CEBS guidelines. In overall, 88% of the jurisdictions incorporated the CEBS concept of 'material activities', i.e. critical, although in a majority of cases (54%) they do not strictly stick 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 reveals that cloud computing is not subject to a specific framework in 14 member states[7] (or 58% of jurisdictions)[8]. In 12 member states (or 50%)[9] some specific frameworks apply. The following activities, either from the CEBS guidelines or from 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 towards the provider
- Full audit rights for the regulated institution

[6] A total of 25 competent authorities from 24 member states participated in the survey.

[7] Please note that the data is based on the survey and as of 18 September 2015, the submission date of the survey responses and bilateral interactions during the time of the production of the consultation paper.

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

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

- Agreement of the regulated institution on the location of the data/services
- Capacity of the regulated institution to re-enter the data/services
- Agreement of the regulate 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, technical requirements by the member states in most cases are not very developed and approximately 50% of the 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 and although similar on some points, each national framework brings its own nuances which do not facilitate the interpretation of the current supervisory expectations in the EU. Without a regulatory intervention the current framework with the above-mentioned shortcoming 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 for competent authorities to apply in their regulatory and supervisory framework for the cloud outsourcing process and the associated risks. Precisely, the recommendations aim to provide the competent authorities with a regulatory framework and tools in their risk assessment and clarity in the process. This is further expected to lead to the harmonisation of the practices and a common level-playing field across jurisdictions. In this way, the current draft recommendations are expected to respond pro-actively to the challenges in the prudential supervision of specific ICT-related risks.

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 the challenges of 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, to reduce uncertainties while providing enough room for flexibility to accommodate the new challenges.	Consistent application of regulatory/supervisory criteria and strengthening prudential supervision.

D. Assessment of the technical options

Introduction of the recommendations vs. 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 the institutions and the competent authorities in their handling 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 the need for further convergence of supervisory practices/expectations was identified or because the areas 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.

In terms of cost of compliance with the recommendations, it is reasonable to expect that the jurisdictions where the current practices overlap or show similarities with what is proposed in the recommendations will bear less administrative cost both for the institutions and the competent authorities. In other words, the more similar are the current practices to the recommendations the less costly will be transition is going to be. The baseline scenario provides some member state level analysis on this aspect.

If a national framework does not comply with the current CEBS guidelines, i.e. CEBS guidelines have not been transposed,[10] the institutions would need to spend more time and resources to:

- produce analyses and information necessary under these recommendations such as the criteria for the materiality assessment (Section 4.1) and the disclosure to supervisors (Section 4.2),
- review legal issues on access and audit rights (section 4.3), and right of access (Section 4.4),
- improve the infrastructure to ensure the appropriate risk assessment, level of protection of data confidentiality, continuity of activities outsources and security, integrity and traceability of data systems (Sections 4.5, 4.6 and 4.7), and
- develop contingency plans and exit strategies (Section 4.8).

Similarly, competent authorities would need to spend more time and resources to process the information received by the institutions.

[10] Notice that this is an assumption and in practice the baseline scenario analysis shows that most member states have either fully or partially in compliance with the CEBS guidelines. If the CEBS guidelines have not been transposed then the member states implement the provisions in their supervisory practices.

However, since most of the 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 vs. non-exhaustive list

Firstly, instead of providing specific guidance for specific types of cloud outsourcing (such as SaaS, IaaS, PaaS), the EBA prefers to introduce as much as possible technology-neutral and future proof recommendations. This would allow a more proactive and flexible framework that would respond more swiftly to the changing context of cloud computing. A more granular guidance would create less flexibility to accommodate the new challenges in the 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 a more prescribed detailed recommendations would limit 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 but within the cybersecurity in general.

Then, the option was taken to include a proportionate approach in the requirements on the exercise by institutions of their right to audit (cloud service providers). Whereas the right to audit needs to be contractually secured, institutions can exercise it in a proportionate manner (for example by organising pooled audits with other customers of the same cloud service providers) to minimise the organisational burden on both the institutions and the 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. It was assessed as overly burdensome from a practical perspective in the context of cloud outsourcing where subcontracting is used extensively, the cloud environment is more dynamic than traditional outsourcing environments, and due to the fact that 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 will have an adverse effect on the risk assessment of the outsourced services).

These preferred technical options are expected to have less administrative cost both for the institutions and the competent authorities. Given the ever developing and 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 would be certainty, reduction in operational risk, level playing field across institutions and supervisory convergence. These benefits are expected to exceed the associated cost of compliance.

5.2 Overview of questions for consultation

1. Are the provisions from these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?

2. Are there any additional areas which should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?