BANCO DE ESPAÑA
Eurosistema

Recommendations on outsourcing to cloud service providers

(EBA/REC/2017/03)

These Recommendations of the European Banking Authority (EBA) 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, i.e credit institutions and investment firms.

The Recommendations build on the guidance provided by the Committee of European Banking Supervisors guidelines on outsourcing (CEBS guidelines), which remain applicable. The Recommendations are not exhaustive, and they should be read in conjunction with the CEBS guidelines.

The purpose of these EBA Recommendations is to specify the supervisory requirements and processes that apply when institutions outsource to cloud service providers. The aims are to 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; and to foster supervisory convergence regarding the expectations and processes applicable in relation to the cloud.

The Recommendations provide directions on how to assess the materiality of cloud outsourcing; include guidance on the process that institutions should follow in informing their competent authorities about material cloud outsourcing and the information to be provided; further explain supervisory expectations on the right to audit for institutions and competent authorities and the right of physical access to the business premises of cloud service providers; include guidance on the security of the data and systems used and address the treatment of data and data processing locations; set 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; and provide guidance for institutions on the contractual and organisational arrangements for contingency plans and exit strategies that should be in place.

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.

These Recommendations have been developed on the EBA's own initiative in accordance with article 16 of Regulation (EU) No 1093/2010. The European Banking Authority published the English version of these Recommendations on 20 December 2017 (the Spanish version was released on 28 March 2018). The Recommendations will apply from 1 July 2018.

The Executive Commission of the Banco de España, in its role of competent authority for the direct supervision of the less significant institutions, adopted these Recommendations as their own on 18 May 2018.

EBA/REC/2017/03

28/03/2018

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.[1] 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 28.05.2018. 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/2017/03'. 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).

[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, (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.[2]

Definitions

3. Unless otherwise specified, terms used and defined in Directive 2013/36/EU[3] 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.

[2] 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.

[3] 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.