ANNEX 1

OUTSOURCING TO CLOUD SERVICE PROVIDERS

Introduction

1. Annex 1 to BR/14 on Outsourcing by Credit Institutions licenced under the Banking Act 1994 ('hereinafter referred to for the purposes of this Annex as 'the Rule') provides additional guidance in the specific context of institutions that outsource to cloud service providers and specifies the supervisory requirements and processes that apply when institutions outsource in this manner.

Scope of Application

2. The scope of this Annex is to implement the Recommendations on Outsourcing to Cloud Service Providers (EBA/REC/2017/03), issued by the European Banking Authority ('EBA') on the 20 December 2017 (hereinafter referred to for the purposes of this Annex as the 'EBA Recommendations'), which build on the guidance provided by the general outsourcing guidelines of the Committee of European Banking Supervisors ('CEBS guidelines'). The EBA Recommendations provide the necessary clarity for credit institutions should they wish to adopt cloud computing while ensuring that risks are appropriately identified and managed.

Definitions

3. For the purposes of this Annex, unless otherwise specified, the following definitions shall apply:

   "*Cloud services*" shall mean 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*" shall mean cloud infrastructure available for open use by the general public.

   "*Private cloud*" shall mean cloud infrastructure available for the exclusive use by a single credit institution.

   "*Community cloud*" shall mean cloud infrastructure available for the exclusive use by a specific community of credit institutions, including several credit institutions of a single group.

"*Hybrid cloud*" shall mean cloud infrastructure that is composed of two or more distinct cloud infrastructures.

Materiality assessment

4. Outsourcing credit institutions shall, prior to any outsourcing of their activities, assess which activities shall be considered as material. Credit institutions shall perform this assessment of activities' materiality on the basis of paragraph 12f of the Rule 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. whether they are activities that are critical to the business continuity/viability of the credit 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 credit institution's revenue prospects;

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

Duty to adequately inform the Authority

5. Outsourcing credit institutions shall adequately inform the Authority of material activities to be outsourced to cloud service providers. Credit institutions shall perform this on the basis of Principle 4.3 of the Rule and, in any case, make available to the Authority the following information:

   a) the name of the cloud service provider and the name of its parent company (if any);

   b) the 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).

6. Further to the information provided in accordance with the previous paragraph, the Authority may ask the outsourcing credit 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 credit institution;

   b) whether the outsourcing credit 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 credit institution maintains the skills and resources necessary to adequately monitor the outsourced activities.

7. The outsourcing credit institution shall 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 shall make available to the Authority, upon 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 credit institution as material.

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

   a) the information referred to in paragraph 5(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 Board of Directors 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 credit 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.

Access and Audit Rights

9. On the basis of paragraph 34(g) of the Rule and for the purposes of cloud outsourcing, outsourcing credit institutions shall 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 credit institution, to any third party appointed for that purpose by the credit institution and to the credit 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 credit institution, to any third party appointed for that purpose by the credit institution and to the credit institution's statutory auditor, unrestricted rights of inspection and auditing related to the outsourced services (right of audit).

10. The effective exercise of the rights of access and audit shall 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 credit institution shall be agreed on.

11. The outsourcing credit institution shall exercise its rights to audit and access in a risk-based manner. Where an outsourcing credit institution does not employ its own audit resources, it shall 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 credit 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 credit 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 credit 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 credit 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 shall be reasonable, and legitimate from a risk management perspective.

12. Considering that cloud solutions have a high level of technical complexity, the outsourcing credit institution shall 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.

13. On the basis of paragraph 34(h) of the Rule and for the purposes of cloud outsourcing, outsourcing credit institutions shall 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 Authority (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 credit institution (right of access);

    b) to confer to the Authority (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).

14. The outsourcing credit institution shall ensure that the contractual arrangements do not impede its Authority to carry out its supervisory function and objectives.

15. Information that the Authority obtains from the exercise of the rights of access and audit shall be subject to the professional secrecy and confidentiality requirements referred to in Articles 25(2), 34(4) and (5) of the Banking Act.

16. Based on the findings of its audit, should any deficiencies be identified, the Authority shall, where necessary, impose any measures, in accordance with the Banking Act, directly on the outsourcing credit institution.

The right of access

17. The agreement referred to in paragraphs 9 and 13 shall include the following provisions:

    a) the party intending to exercise its right of access (institution, the Authority, auditor or third party acting for the credit institution or the Authority) shall, before a planned onsite visit, provide notice within 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 Authority, as well as the credit institution and its auditor, in connection with the onsite visit.

Security of data and systems

18. As stated by paragraph 34(e) of the Rule, the outsourcing contract shall oblige the outsourcing service provider to protect the confidentiality of the information transmitted by the financial institution. In line with paragraph 31(e) of the Rule, credit institutions implement arrangements to ensure the continuity of services provided by outsourcing service providers. Building on paragraph 34(b) and Principle 9 of the Rule, the respective needs of outsourcing credit institutions with respect to quality and performance shall feed into written outsourcing contracts and service level agreements. These security aspects shall also be monitored on an ongoing basis.

19. For the purposes of the previous paragraph, the credit institution shall 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, integrity, traceability of data and systems in the context of the intended cloud outsourcing. Credit institutions shall 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.

20. Subsequently, credit institutions shall 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 19(c) are set out.

21. Credit institutions shall monitor the performance of activities and security measures in line with Principle 7 of the Rule, including incidents, on an ongoing basis and review as appropriate whether their outsourcing of activities complies with the previous paragraphs; they shall promptly take any corrective measures required.

Location of data and data processing

22. As stated in paragraph 22 of the Rule, credit institutions shall 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 Authority.

23. The outsourcing credit institution shall adopt a risk-based approach to data and data processing location considerations when outsourcing to a cloud environment. The assessment shall 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 shall 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 jurisdiction, including the insolvency law provisions that would apply in the event of a cloud service provider's failure. The outsourcing credit institution shall ensure that these risks are kept within acceptable limits commensurate with the materiality of the outsourced activity.

Chain outsourcing

24. As stated in Principle 10 of the Rule, credit institutions shall take account of the risks associated with 'chain' outsourcing, where the outsourcing service provider subcontracts elements of the service to other providers. The outsourcing credit institution shall agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing credit institution and the outsourcing service provider. Furthermore, the outsourcing credit institution shall 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.

25. The outsourcing agreement between the outsourcing credit institution and the cloud service provider shall 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.

26. The outsourcing agreements shall also include an obligation for the cloud service provider to inform the outsourcing credit 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 shall be contractually pre-agreed to allow the outsourcing credit 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.

27. 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 credit institution shall have the right to terminate the contract.

28. The outsourcing credit institution shall 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.

Contingency plans and exit strategies

29. As stated in Principle 6.1 and paragraphs 31(e) and 34(d) of the Rule, the outsourcing credit institution shall 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 shall include contingency planning and a clearly defined exit strategy. Furthermore, the outsourcing contract shall 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.

30. An outsourcing credit institution shall 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 credit institution shall:

    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 credit institution in the event of the termination of the outsourcing agreement.

31. When developing exit strategies, an outsourcing credit institution shall 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.

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