Baker McKenzie.

Financial Services
June 2017

Client Alert

June 2017
For more information please contact:

Arun Srivastava
+44 20 7919 1285
arun.srivastava@bakermckenzie.com

Mark Simpson
+44 20 7919 1403
mark.simpson@bakermckenzie.com

The EBA's draft Recommendations for Cloud Outsourcing

The European Banking Authority (EBA) published a Consultation Paper on 17 May 2017 setting out draft Recommendations on outsourcing by financial institutions to cloud service providers.[1] This will be open for consultation until 18 August 2017 and a public hearing on the consultation will take place on 20 June 2017 at the EBA's offices in Canary Wharf.

Cloud outsourcers provide IT resources such as servers, storage, databases and applications via the Internet. They own and maintain data centre facilities housing the infrastructure to offer these services, although they can sub-contract with third parties known as "chain outsourcing".

2006 CEBS Guidelines

The draft Recommendations supplement the CEBS Guidelines published by the EBA's predecessor in 2006.[2] Since then, the volume of financial information and data created by firms and demand for outsourcing to cloud service providers has increased very substantially. The EBA states that without additional guidance the CEBS Guidelines will fail to provide an adequate regulatory framework for firms and supervisors to handle cloud outsourcing activities in the banking sector. Although most Member States have transposed the CEBS Guidelines, the EBA is also concerned that implementation varies across jurisdictions. The EBA has chosen not to provide guidance for specific types of cloud outsourcing,[3] but to introduce so far as possible "technology-neutral" and "future proof" recommendations.

Two key issues of commercial importance to cloud service providers are the so called "right of audit" and chain outsourcing.

Audit & Access Rights

There is considerable concern in the industry over the extent and reach of

Nina Moffatt
+44 20 7919 1081
nina.moffatt@bakermckenzie.com

Richard Powell
+44 20 7919 1577
richard.powell@bakermckenzie.com

the right of audit (and access) granted to financial sector firms and regulators over cloud service providers. This is particularly acute where data centres are multi-tenanted or have a "shared environment" for a range of customers. Suppliers are understandably anxious to limit audit rights so that they do not intrude on the services provided to other clients.

While the Financial Conduct Authority's (FCA) Finalised Guidance on Outsourcing to the Cloud explains its expectations, the EBA's draft Recommendations set out in far more detail the nature of the rights required to be contractually incorporated. Cloud service providers will not be able to push back completely on the principle of access and audit. Rather, the question is how to best manage these demands and minimise the consequent disruption and risk (especially to other clients).

In this regard, the EBA is conscious of suppliers' concerns and the fact that it expects financial institutions to adopt a risk-based approach when complying with the draft Recommendations is to be welcomed.

In this regard, as referred to below under Guideline 8, the draft Recommendations put forward a number of alternatives to a client exercising rights of access and audit. For example, by use of "pooled audits" with other clients of the same supplier, certifications of compliance provided by an independent third party, or internal reports from the outsourcers themselves (subject to safeguards). In principle, this flexibility is a positive development, although much will depend on how national regulators respond to these solutions.

Chain Outsourcing

With respect to chain outsourcing, the EBA considers that there is a need to improve certainty about the conditions under which subcontracting is permitted. The draft Recommendations mandate the concept of "flow down" to ensure that the risks associated with sub-contracting are kept to a minimum. Similarly, to see that continuity of service is robust, financial institutions must carry out appropriate risk assessments and service agreements should allow for termination where there is concern over the potential for an adverse impact on services. Clearly, this will have cost implications as cloud providers and their chain outsourcers will lose some flexibility and need to carry additional resource.

UK Requirements / Guidance

In the UK, requirements for structuring outsourcings are contained in chapter 8 of the FCA's Senior Management Arrangements, Systems and Controls Sourcebook (SYSC) that applies as rules to MiFID and CRD firms and as guidance to all others.

With respect to outsourcing to the "cloud", the FCA published Finalised Guidance in 2016, which while not binding on firms requires them to take note of, and serves to illustrate how they can comply with regulatory requirements.[4] There is considerable overlap between the FCA's Finalised Guidance on the Cloud and the EBA's draft Recommendations. The PRA has also published a supervisory statement on resolution planning which also concerns outsourcing that is relevant to dual-regulated firms.[5]

Draft EBA Recommendations

Set out below, in blue, are the CEBS Guidelines supplemented, where relevant, by a summary of the draft Recommendations which need to be read and understood in the light of the former.

Guideline 1

This contains definitions such as for "outsourcing" where an authorised

entity's use of a third party to perform activities that would normally be undertaken by the authorised entity, now or in the future. The supplier may itself be an authorised or unauthorised entity.

Guideline 2

The ultimate responsibility for the proper management of the risks associated with outsourcing or the outsourced activities lies with an outsourcing institution's senior management.

Guideline 3

Outsourcing arrangements can never result in the delegation of senior management's responsibility.

Guideline 4

4.1 An authorised entity may not outsource services and activities concerning the acceptance of deposits or to lending requiring a licence from the supervisory authority according to the applicable national banking law unless the outsourcing service provider either (i) has an authorisation that is equivalent to the authorisation of the outsourcing institution; or (ii) otherwise allowed to carry out those activities in accordance with the relevant national legal framework.

4.2 Any area of activity of an outsourcing institution other than those identified in Guidelines 2 and 3 may be outsourced provided that such outsourcing does not impair: [for example, a range of criteria including management's ability to manage and monitor].

4.3 An outsourcing institution should take particular care when outsourcing material activities. The outsourcing institution should adequately inform its supervisory authority about this type of outsourcing.

Prior to outsourcing activities firms should consider which activities are material and carry out an assessment on the basis of the CEBS Guidelines. Specifically, they should take into account the: (1) criticality and inherent risk profile of activities (2) operational impact of outages (3) impact any disruption would have on prospective revenue, and (4) the impact of a confidentiality breach or a failure of "data integrity".

Where "material" activities are being outsourced firms must "adequately" inform their supervisors. The draft Recommendations list the information to be provided. A firm should keep a register with information on all its material and non-material outsourced activities at firm and group level - the content of which is prescribed in the draft Recommendations. The supervisor may ask to see the records and any relevant outsourcing agreements.

Special care on the basis of a risk based analysis should be exercised with cloud service providers outside the EEA because of data protection risks and the difficulties regarding "effective supervision." Firms should prepare a written assessment covering the potential impacts, legal risks and compliance issues, and oversight difficulties.

Guideline 5

There should be no restrictions on the outsourcing of non-material activities of an outsourcing institution.

Guideline 6.2

6.1 The outsourcing institution should have a policy on its approach to outsourcing, including contingency plans and exit strategies.

6.2 The outsourcing institution should have a policy on its approach to

outsourcing, including contingency plans and exit strategies.

Supervisors may ask for information on whether there is a suitable business continuity plan (BCP), an exit strategy (should there be a need to change the cloud service provider), and if the firm has the skills and resources necessary to adequately monitor the outsourced activities. This will include the development of key risk indicators to flag up unacceptable service levels.

In the context of BCP etc., the agreement between the firm and the cloud service provider must include a termination and exit management clause permitting transfer of the provision of the activities to another provider or their return to the firm. It should be possible to carry out this step without undue disruption to their provision of services and to achieve this proper planning must be undertaken, alternative solutions identified and the contractual position aligned.

Guideline 7

An outsourcing institution should manage the risks associated with its outsourcing arrangements.

The agreement with the cloud service provider must require it to keep confidential information sent to it. This should be reflected in the agreement and monitored on a regular basis.

Prior to outsourcing a firm should (1) identify and classify its activities, processes and related data and systems as to the sensitivity and required protections needed, (2) conduct a risk-based review of those activities which are to be outsourced, and (3) arrive at appropriate levels of protection for data confidentiality, continuity of activities and the integrity and traceability of data and systems.

Firms should monitor the performance of activities and security measures including incidents, on an on-going basis.

Guideline 8

All outsourcing arrangements should be subject to a formal and comprehensive contract. The outsourcing contract should oblige the outsourcing service provider to protect confidential information.

Firms must have written agreements in place with the cloud service provider that provide the firm, its agents, auditors and supervisors with full access to business premises and all devices, systems, networks and data. Accompanying this "right of access" must be a similar "right of audit" to inspect and audit. Such rights should not be impeded by the contract, but must be used in a risk-based manner.

In this regard, reflecting the concerns of suppliers, the draft Recommendations provide that where the exercise of one client's rights to access and audit may create risks for other clients of the provider, alternative means of providing the necessary level of comfort should be explored.

Moreover, if a firm does not have an audit capability it may enter into a shared or pooled arrangement with other firm(s) or potentially (subject to limitations) rely on third-party certifications and third party, or even internal reports from the cloud service provider subject to safeguards. The firm must ensure that its staff carrying out the audit or reviewing third-party certifications have the right skills and knowledge to do so.

Guideline 9

In managing its relationship with an outsourcing service provider an outsourcing institution should ensure that a written agreement on the

responsibilities of both parties and a quality description is put in place.

Guideline 10

10.1 The outsourcing institution should take account of the risks associated with "chain" outsourcing.

10.2 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, including obligations incurred in favour of the supervisory authority.

10.3 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.

Chain outsourcing refers to subcontracting by the cloud service provider. Firms should only agree to this practice if the subcontractor accepts the same obligations as the primary provider. The principal agreement between the firm and the cloud service provider should require the firm to be informed in advance to allow time to carry out a risk assessment and, if it concludes that there will be an adverse impact on the services in question, to terminate the agreement. Additionally, the agreement should specify what activities cannot be subcontracted.

Guideline 11

Supervisory authorities should require that the outsourcing institution has established supervisory authority access to relevant data held by the outsourcing service provider and, where provided for by the national law, the right for the supervisory authority to conduct onsite inspections at an outsourcing service provider's premises.

Guideline 12

Supervisory authorities should take account of concentration risk.

---

[1] See EBA/CP/2017/16.

[2] Guidelines on Outsourcing, Committee of European Banking Supervisors, 14 December 2006.

[3] For example, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

[4] FCA, Finalised Guidance FG 16/5 - Guidance for Firms Outsourcing to the 'Cloud' and Other Third-party IT Services, July 2016.

[5] PRA, Supervisory Statement (SS19/13) Resolution Planning, December 2013.