FCA Consultation on Cloud - Response
Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary University of London

Submission by Dr Kuan Hon w.k.hon@qmul.ac.uk, Prof Christopher Millard c.millard@qmul.ac.uk, and Prof Ian Walden i.n.walden@qmul.ac.uk

11 February 2016

1. Introduction

We welcome the FCA's aim of balancing risk management against innovation, its acknowledgement that there is no fundamental reason why public cloud services cannot be implemented compliantly with FCA rules, its cost benefit analysis and its intention to monitor the impact of cloud outsourcing on competition in financial services and how its guidance will be used in practice.

2. General comments

The highly granular and prescriptive model that is proposed is likely to be disadvantageous to cloud providers that offer specialist services to firms using third party cloud platforms or infrastructure. Global, vertically integrated, cloud providers are more likely to have the expertise and resources necessary to satisfy the requirements as compared to specialist UK or other European providers. This may have a chilling effect on both innovation and competition.

It is also important to bear in mind that there are fundamental differences between cloud and traditional outsourcing models (please see http://www.scl.org/site.aspx?i=ed28054 and, for a longer version, http://ssrn.com/abstract=2200592). For the FCA's guidance to be workable and appropriate, it needs to take these differences into account.

3. Detailed comments

We agree that a risk-based and proportionate approach needs to be taken to cloud, with particular reference to the type(s) of function(s) being outsourced to cloud.

P. 8 Legal and regulatory considerations – "know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the United Kingdom. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and regulator (see below sections on access to data and business premises)". These are two separate issues, and should be dealt with separately. A contract may be governed by English law and subject to the jurisdiction of the English courts, yet still not ensure effective access to data or premises. Furthermore, we consider that access for the firm or its auditor should be dealt with separately from access for the regulator, because the latter can raise sovereignty and public law enforcement issues that do not arise with the firm/auditor.

P. 8 Legal and regulatory considerations – "identify all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain." It may be possible for requirements on the firm to be complied with even if it does not know all the service providers in the supply chain, for example because its direct service provider (such as a cloud provider) has assumed liability for the performance of its sub-providers and has taken appropriate steps to manage the risk of sub-providers' failures. In outsourcing situations not involving cloud, as long as the service provider can carry out the outsourced services effectively, it should not be necessary to identify all service providers involved. So too with cloud. For example, with a non-cloud outsourcing service provider, must all service providers in the supply chain always be identified such as third party data centres and connectivity/network service providers? The answer is that it depends on the circumstances. A rigid rule that all possible service providers in the chain must be identified when using cloud services may discriminate against cloud. What is important is ensuring

requirements on the firm can be complied with throughout the supply chain. To achieve this objective may not always require identifying all possible service providers involved.

P. 9 Risk management – "review whether the legal and regulatory risks differ if the customers, firms and employees involved in providing or using the services are in different geographic or jurisdictional locations e.g. UK, EEA or non-EEA". Issues regarding processing of data in different geographic or jurisdictional locations would be more relevant to this area than to security, and we recommend that they be moved here (see later, P. 10 Data security).

P. 9 Risk management – "require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements". Requiring notification of "any" breaches may be too broad and lead to "notification fatigue" if immaterial minor breaches must be notified. We recommend qualifying this requirement by reference to the materiality/relevance of the breach to the firm concerned, and clarifying what are "breaches" for this purpose, e.g. only breaches of confidentiality, integrity or availability?

P. 9 Risk management – "ensure the contract(s) provide for the remediation of breaches and other adverse events". The degree of control (and therefore responsibility) retained or maintained by the firm depends on the type of cloud service. For example, with IaaS or PaaS, the firm would have significant control over many aspects of its service use, and therefore responsibility for certain breaches may lie with the firm rather than the cloud provider. It should not be assumed that all breaches are caused by, and must be remediated by, cloud providers.
P. 9 International standards – reference might be added here to cloud-specific standards such as ISO 27017 and 27018, the Cloud Security Alliance's Cloud Controls Matrix, and the Cloud Industry Forum's Code of Practice.

P. 10 Oversight of service provider "allocate responsibility for the day-to-day and strategic management of the service provider"– very minor point, suggest adding "internal" before "responsibility".

P. 10 Data security "have a data residency policy that sets out where data can be stored… have choice and control regarding the jurisdiction in which their data is stored, processed and managed" – these are issues regarding jurisdiction to regulate the processing of the firm's data (including compelled disclosures of data to authorities). They would be dealt with more appropriately under Legal and regulatory considerations, above. If data are strongly-encrypted and backed up, then their "residency" should be irrelevant to their security. Thus, whether a data residency policy is important should depend on the individual circumstances. As for choice and control regarding jurisdictions of data processing, many cloud providers process certain data in one jurisdiction, and other data in others, so that firms may have such choice and control only regarding certain data (for example see https://www.microsoft.com/en-us/TrustCenter/Privacy/You-are-in-control-of-your-data/Azure-location under "Data storage for regional services" and "Data storage for global services"). However, provided there is transparency for firms regarding the data over which they have no choice or control regarding jurisdictions, and they have assessed the risks accordingly, there seems no reason why there should be an absolute rigid requirement that firms must have choice and control of jurisdictions of all possible data involved in the service.

P. 10 Data security "consider data sensitivity and how the data is transmitted, stored and encrypted, where necessary" – suggest adding, after "encrypted", "whether in transmission or in storage".

P. 11 Effective access to Data "ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive" – does "notification requirements on accessing data" mean, "pre-conditions regarding notifications to the service provider before the firm can access data"? Clarification would be helpful. Furthermore, note that by their nature cloud services involve direct self-service usage by customers, including viewing or downloading their data and/or logs without the need to notify or even involve the cloud provider.

P. 11 Effective access to Data "ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data" – SYSC 8.1.8(9) only requires "effective" access to data. Access may be "effective" even if there are some restrictions, e.g. to a reasonable number or frequency of requests. Requiring "no" restrictions at all seems too rigid and extreme, going

beyond the base regulatory requirement, and cloud providers may well refuse to agree to this requirement, for reasons of security and practicability.

P. 11 Effective access to Data "ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly" – if there are legally-binding reasons why a firm cannot disclose data to its regulator or auditor, it may well be that the service provider might also be prohibited by law from disclosing such data. Such a contractual requirement therefore may not be fair or indeed legally possible for the provider to comply with.

P. 11 Access to business premises – "assess" should be "access". More substantively, we welcome the FCA's recommendation to focus on business premises that are relevant for effective oversight, and its recognition that service providers may, for legitimate security reasons, need to limit access to some sites.

P. 11 Access to business premises – Firm and auditor access "A firm should be able to request an onsite visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. This right should not be restricted." Please see above (restrictions on requests for data) – "effective" access to premises is not the same as "unrestricted" access to premises, and unrestricted onsite visits seems to go beyond "effective" access, as indeed is recognised by the later statements "A firm can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation" and "The regulator can commit to visits occurring during business hours and at a time specified by the outsourcing provider or with reasonable notice, except in an emergency or crisis situation".

[P. 12 Access to business premises - Regulator access "During the visit, the regulator should be permitted to view the provision of services to the regulated firm or any affiliate within the group, as required under applicable financial services legislation. The regulator can commit to minimising, disruption to outsourcing providers' operations" – the opportunity "to view the provision of services to the regulated firm or any affiliate" may be appropriate in a business process outsourcing, but will make little sense in most cloud service arrangements due to their "self-service" nature.

P. 12 Relationship between service providers "If the regulated firm does not directly contract with the outsource provider, it should review sub-contracting arrangements to determine whether these enable the regulated firm to continue to comply with its regulatory requirements. Firms should consider, for example, security requirements and effective access to data and business premises. The regulated firm must be able to comply with these regulatory requirements even if it does not directly contract with the outsource provider" – please see above regarding supply chain – individual circumstances may vary considerably, and a firm may be able to comply even if it does not review all sub-contracting arrangements: indeed, the guidance states, "The regulated firm should consider how service providers work together. For example will the firm or one service provider take the lead systems integration role?". With a non-cloud outsourcing, a firm may not always need to review all sub-contracts such as with connectivity providers, and cloud outsourcing should not be subjected to additional requirements unless warranted by the risks and context, i.e. a rigid rule regarding review of sub-contracting arrangements seems to discriminate against cloud.

P.14 Exit plan "have a specific obligation put on the outsourcing provider to cooperate fully with both the firm and any new outsource provider(s) to ensure there is a smooth transition" – it may be difficult to persuade cloud providers to agree to "fully" rather than, for example, "to the fullest extent reasonable subject to payment of costs/charges".

P.14 Exit plan "know how it would remove data from the service provider's systems on exit" – we would suggest changing this to "remove and delete data as quickly and effectively as needed…".

4. Cloud Legal Project

The Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London, has been researching legal issues in cloud computing since 2009, led by Prof Christopher Millard. Publications include *Cloud Computing Law* (OUP 2013), Millard (ed).