Financial Conduct Authority

Guidance consultation 15/6

Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services

November 2015

1. Introduction and consultation

1.1 The purpose of this draft guidance is to clarify the requirements on firms[1] when outsourcing to the 'cloud' and other third-party IT services. This guidance is broader than, but includes issues covered in, 'Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions', which we published in July 2014 as part of our barriers-to-entry work for firms entering, or considering entering, the banking sector. While the July 2014 publication focused on banking solutions, this guidance is intended to help all firms to effectively oversee all aspects of the life cycle of their outsourcing arrangements: from making the decision to outsource, selecting an outsource provider, and monitoring outsourced activities on an ongoing basis, through to exit.

1.2 In October 2014, the Financial Conduct Authority (FCA) launched Project Innovate – an FCA initiative to foster innovation in financial services. One of the main differences between the FCA and the FSA is that we have an objective to promote effective competition. Innovation can be a driver of effective competition, so we want to support innovation and ensure that regulation unlocks these benefits, rather than blocks them. In producing this guidance, we have worked closely with Project Innovate to identify areas where our regulatory framework needs to adapt to enable further innovation in the interests of consumers.

[1] We believe this guidance will be of interest to all firms dealing with the FCA, including those authorised under Part 4A of the Financial Services and Markets Act 2000 (FSMA) and those licensed under other regimes, such as the E-Money Regulations 2011. However, firms should ensure they comply with the specific requirements that apply to them based on their status.

1.3 Stakeholders including firms and cloud service providers have told us that they are unsure about how we apply our rules relating to outsourcing to the cloud. Through roundtable discussions and other interactions with firms and cloud service providers; we understand that this uncertainty may be acting as a barrier to firms using the cloud.

1.4 'Cloud' is a broad term, and stakeholders have interpreted it differently. The FCA sees the cloud as encompassing a range of IT services provided in various formats over the internet. This includes, for example, private, public or hybrid cloud, as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud services are constantly evolving. Our aim is to avoid imposing inappropriate barriers to firms' ability to outsource to innovative and developing areas, while ensuring that risks are appropriately identified and managed.

1.5 There are particular risks associated with outsourcing to the cloud which differ from traditional outsourcing arrangements, and these risks primarily affect the degree of control exercised by the firm.

a. Cloud customers may have less scope to tailor the service provided.

b. Cloud customers may also have to accept that cloud service providers will move their data around; however, in some cases, cloud customers may be able to specify which overall geographic region in which their data is stored.

c. Firms should also consider the risks associated with outsource service providers who may contract out part of their operation to other cloud providers. This may occur without the firm initially realising.

1.6 We are therefore setting out in more detail our approach to regulating firms who outsource to the cloud and other third-party IT services. We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.

1.7 Firms should also be aware of international developments taking place that are likely to have an impact on their decision-making process regarding the use of cloud services: notably, the new EU Digital Single Market strategy and reform of EU Data Protection legislation. These are evolving areas and the FCA is engaging in this work as proposals are developed. As such, firms and service providers should continue to monitor EU developments and the impact on their business.

1.8 We are required to consult on this guidance because it constitutes 'guidance on rules'. This guidance is not binding, however we expect firms to take note of the guidance and, where appropriate, use it to inform their systems and controls on outsourcing.

1.9 The guidance is not exhaustive, nor should it be read in isolation. Firms should consider this guidance in the context of their overarching obligations under the regulatory system. The FCA, based on its statutory objectives, is of the view that complying with this guidance will generally indicate compliance with the aspects of the FCA rule or other requirement to which the guidance relates, though it is not exhaustive. The PRA has different statutory objectives, and so firms that are subject to PRA regulation should

confirm their approach with the PRA. FCA guidance on rules, the Act or other legislation represents the FCA's view, and does not bind the PRA or the courts.

1.10 We are consulting on this guidance for three months and welcome any comments you may have. You can send your response by email to **itoutsourcing@fca.org.uk**

1.11 Please respond by 12 February 2016.

1.12 Following consultation, we intend to publish the final guidance on our website.

2 Who does this guidance affect

2.1 The purpose of this guidance is to help firms and service providers understand the FCA's expectations where firms are using, or are considering using, the cloud and other third-party IT services.

2.2 This guidance will be of particular interest to firms interested in outsourcing to the cloud and other third-party IT services. The guidance may also be of interest to:

a. third-party IT providers, including cloud providers, seeking to provide services to financial services firms
b. trade associations and consumer groups
c. law firms and other advisers, and
d. auditors of financial services firms

3 Cost benefit analysis

3.1 Section 138I of the Financial Services and Markets Act (FSMA) requires us to perform a cost benefit analysis (CBA) of our proposed requirements and to publish the results, unless we consider the proposal will not give rise to any cost or to an increase in costs of minimal significance.

3.2 Through discussions with stakeholders, including new entrants seeking authorisation and cloud service providers, we have been working to identify areas where our regulatory framework needs to adapt to enable further innovation in the interests of consumers. Firms outsourcing, or considering outsourcing, to the cloud and other third party IT services have told us that how we view the cloud and how they should comply with our rules on outsourcing is important to them. This guidance aims to help firms understand our expectations and comply with our existing rules, including the FCA's approach to outsourcing to the cloud and third party IT services.

3.3 The use of outsourcing to the cloud and other third party IT services can have a positive impact on competition in financial services, in so far as they can facilitate entry and/or expansion, and increase the ability of financial services providers, overall, to renew their IT systems in a more efficient manner. However, there may be also potential

competition risks related to the economies of scale and scope associated with cloud services that could result (in the medium and long-run) in constraints or limited choice for users, the impact of which needs to be monitored and taken into consideration.

3.4 If firms alter their approaches to engaging or overseeing outsourced services in response to our proposed guidance the benefits and costs associated with outsourcing will be impacted. However, by clarifying our existing expectations we do not consider that costs will rise materially overall as a clearer understanding of our expectations should allow firms to us make more effective use of outsourcing where this is appropriate. We also expect benefits to accrue through improved choice and innovation in outsourcing, with commensurate benefits for firms and consumers.

3.5 As the use of outsourcing to the 'cloud' and other third party IT services is dynamic and uncertain we consider that it will be important to monitor how the guidance is being used by firms and other stakeholders so as to assess its potential impact on the market and its development. Consequently, we invite feedback on the costs and benefits of these proposals.

4 Compatibility statement

4.1 Section 1B of FSMA requires the FCA, when discharging its general functions, as far as is reasonably possible, to act in a way that is compatible with its strategic objective and advances one or more of its operational objectives. The FCA also needs to, so as far as is compatible with acting in a way that advances the consumer protection objective or the integrity objective, carry out its general functions in a way that promotes effective competition in the interests of consumers.

4.2 We are satisfied that these proposals are compatible with our general duties under section 1B of FSMA, having regard to the matters set out in 1C(2) FSMA and the regulatory principles in section 3B.

4.3 In preparing the proposals as set out in this consultation, we have considered the FCA's duty to promote effective competition in the interests of consumers. We do not consider these amendments are likely to have any adverse impact on effective competition.

4.4 The proposed changes are not expected to have a significantly different impact on mutual societies.

5 Equality and diversity

5.1 We have considered the equality and diversity issues that may arise from these proposals. Overall, we do not consider that the proposals raise concerns with regards to equality and diversity issues.

5.2 We do not consider that the proposals in this consultation adversely impact any of the groups with protected characteristics, i.e., age, disability, sex, marriage or civil partnership, pregnancy and maternity, race, religion and belief, sexual orientation and gender reassignment.

5.3 We will continue to consider the equality and diversity implications of the proposals during the consultation period, and will revisit them when publishing the final guidance. In the interim we welcome any feedback to this consultation on such matters.

6 Consultation guidance for firms outsourcing to the cloud and other third-party IT services

Introduction

6.1 A firm has many choices when designing its operating model and setting its IT strategy. It may choose to develop and operate its own services or use a third party to cater to some or all of its needs. This market continues to evolve rapidly, with frequent new offerings and innovative ways of delivering these services.

6.2 The use of third-party providers to deliver services for regulated firms can bring benefits to firms, their consumers, and the wider market. However, it can also introduce risks that need to be identified, monitored and mitigated.

6.3 This guidance includes a list of several areas that a firm should consider during its preparations for the use, evaluation and ongoing monitoring of third parties in the delivery of IT services that are essential to the effective functioning of the regulated firm's business operations.

6.4 This guidance is not exhaustive, nor should it be read in isolation. Firms should consider this guidance in the context of their overarching obligations under the regulatory system. The FCA, based on its statutory objectives, is of the view that complying with this guidance will generally indicate compliance with the aspects of the rule or requirement to which the guidance relates. The Prudential Regulatory Authority (PRA) has different statutory objectives, and so firms that are also subject to PRA regulation should confirm their approach with the PRA. FCA guidance on rules, the Financial Services and Markets Act 2000 or other legislation represents the FCA's view, and does not bind the PRA or the courts.

Cloud computing

6.5 As noted above, the term 'cloud' encompasses a range of different IT services. Each service has features and risks associated with it, and it is for firms to consider which outsourcing option is the best fit for their business. From a regulatory perspective, the exact form of the service used does not, in itself, alter the regulatory obligations placed on firms. It is important to note that where a third party delivers services on behalf of a regulated firm – including a cloud provider – this is considered **outsourcing** and firms need to consider the relevant regulatory obligations and how they comply with them. This guidance is intended to assist firms in meeting their regulatory requirements when outsourcing to third-party IT services, including the cloud.

Outsource service regulatory requirements

6.6 The overall aim of the high-level regulatory obligations on outsourcing, and the detailed requirements that underpin them, is that a firm appropriately identifies and manages the operational risks associated with its use of third parties, including undertaking due diligence before making a decision on outsourcing. Our approach is risk-based and

proportionate, taking into account the nature, scale and complexity of a firm's operations. Regulated firms retain full responsibility and accountability for discharging all of their regulatory responsibilities. Firms cannot delegate any part of this responsibility to a third party.

6.7 Firms should note that different requirements apply to different types of firm (many of which derive from EU legislation) and may be determined by the type of function being outsourced. However, the outcome they are expected to demonstrate and evidence will be the same. Of particular relevance is whether or not the function being outsourced is considered **critical or important**, whether it is **material** outsourcing, or (for authorised payment institutions and authorised electronic money institutions) whether it relates to **important operational functions**. These are specific terms in respect of outsourcing and are defined in the Handbook or Regulations as follows:

- *Critical or important* – an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a common platform firm with the conditions and obligations of its authorisation, its other obligations under the regulatory system, its financial performance, or the soundness or continuity of its relevant services and activities (Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R)).[2]

- *Material outsourcing* – defined in the FCA Handbook as outsourcing services of such importance that weakness or failure of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Principles for Businesses (PRIN).[3]

- *Important operational functions* – under the Electronic Money Regulations 2011 and the Payment Services Regulations 2009, an operational function is important if a defect or failure in its performance would materially impair: (a) the authorised institutions compliance with the Regulations and any requirement of its authorisation; (b) the financial performance of the authorised institution; or (c) the soundness or continuity of the authorised institution. We have published documents that describe our approach to interpreting and applying the regulations, including in relation to outsourcing.[4][5]

6.8 The PRA has also published a supervisory statement on resolution planning which is relevant to dual-regulated firms.[6] This contains information needed to support the PRA's preferred resolution strategy, while ensuring that 'critical economic functions' are maintained. The PRA is also undertaking work on operational continuity and, the requirement to ensure continuity of critical shared services in resolution[7].

[2] Senior Management Arrangements, Systems and Controls (SYSC)
[3] Principles for Businesses (PRIN)
[4] The FCA's role under the Payment Services Regulations 2009
[5] The FCA's role under the Electronic Money Regulations 2011
[6] Supervisory Statement | SS19/13, Resolution Planning
[7] Ensuring operational continuity in resolution – CP38/15

Areas that firms should consider in relation to outsourcing to the cloud and other third-party IT services

The table below sets out areas for firms to consider in outsourcing, including how they should discharge their oversight obligations.

Area of interest	Notes
Legal and regulatory considerations	Before acceptance, firms should review the contract with the outsource provider to ensure that it complies with our rules. A firm should: • have a clear and documented business case or rationale in support of the decision to use one or more service providers for the delivery of critical or important operational functions or material outsourcing • ensure the service is suitable for the firm and consider any relevant legal or regulatory obligations, including where a firm is looking to change their existing outsourcing requirements • as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not erode, impair or worsen the firms operational risk • consider the relative risks of using one type of service over another e.g. public versus private 'cloud' • maintain an accurate record of contracts between the firm and its service provider(s) • know which jurisdiction the service provider's business premises are located in and how that affects the firm's outsource arrangements • 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) • consider any additional legal or regulatory obligations and requirements that may arise such as through the Data Protection Act 1998 (DPA) • 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. Similarly, where multiple providers form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement

Risk management	A fundamental principle of the rules and guidance on outsourcing is that firms identify and manage any risks introduced by their outsourcing arrangements. Accordingly firms should: • carry out a risk assessment to identify relevant risks and identify steps to mitigate them • document this assessment • identify current industry good practice, including data and information security management system requirements, as well as the relevant regulator's rules and guidance to then use this to support its decision making • 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 • assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them • monitor concentration risk and consider what action it would take if the outsource provider failed • require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements • ensure the contract(s) provide for the remediation of breaches and other adverse events.
International standards	In conducting its due diligence on potential third-party providers, and as part of ongoing monitoring of service provision, a firm may wish to take account of the provider's adherence to international standards as relevant to the provision of IT services. Assurance obtained from international standards for the delivery of critical or important operational functions or material outsourcing is unlikely to be sufficient on its own. Nevertheless firms should: • take account of any external assurance that has already been provided when conducting their own due diligence. External assurance may be more relevant to a firm's consideration where: • it complies to well-understood standards (such as, for example, the ISO 27000 series) • the part of the service being assessed is relatively stable (such as physical controls in the data centre or staff vetting)

	• the service is uniform across the customer base (i.e. not particular or bespoke to the firm outsourcing) • the scope of the third-party audit is specific to the service a firm proposes to use (i.e. the audit is against the data-centre you are using – not a similar datacentre in another jurisdiction)
Oversight of service provider	Firms retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider. At a high level, a firm should: • be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends • allocate responsibility for the day-to-day and strategic management of the service provider • ensure staff have sufficient skills and resources to oversee and test the outsourced activities; identify, monitor and mitigate against the risks arising; and properly manage an exit or transfer from an existing third-party provider • verify that suitable arrangements for dispute resolution exist
Data security	Firms should carry out a security risk assessment that includes the service provider and the technology assets administered by the firm. A firm should: • have a data residency policy that sets out where data can be stored • understand the provider's data loss and breach notification processes and ensure they are aligned with the firm's risk appetite and legal or regulatory obligations • have choice and control regarding the jurisdiction in which their data is stored, processed and managed • consider how data will be segregated (if using a public cloud) • take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable • consider data sensitivity and how the data is transmitted, stored and encrypted, where necessary.
Data Protection Act 1998	A firm should comply with the eight principles of the (DPA) and any associated guidance. Data protection requirements are separate from FCA Handbook requirements and each must be met separately. The DPA is overseen and regulated by the Information

	Commissioner's Office (ICO). Firms should therefore follow the ICO's guidance on cloud computing: https://ico.org.uk/for-the-public/online/cloud-computing and other relevant guidance.
Effective access to Data	Specific regulatory requirements for some firms (e.g. SYSC 8.1.8(9)) require effective access to data for regulated firms, their auditors and for regulators. The term "data" has a wide meaning. It includes but is not limited to firm, personal customer and transactional data, but also system and process data: for example Human Resource vetting procedures or system audit trails and logs. A firm should: • ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive. • ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data • advise the service provider that the regulator will not enter into a non-disclosure agreement with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in the Financial Services and Markets Act (FSMA), sections 348 to 349 • 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
Access to business premises	Specific regulatory requirements for some firms (e.g. SYSC 8.1.8(9)) require access, including physical (on-site) access, to business premises of third-party providers for regulated firms, their auditors and for regulators. We regard 'business premises' as a broad term, encompassing a range or premises including: for example, head offices, operations and data centres. For firms where these requirements apply as rules, their contracts must allow for access - including physical assess - to business premises. The focus should therefore be on which business premises are relevant for the exercise of effective oversight; this does not necessarily require access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites – such as data centres. Particular considerations include: **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.

	• A firm can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation. • A firm may elect its auditor to undertake the visit. Note that this must be the firm's auditor and not an auditor appointed by the outsourcing provider. • The scope of the firm and/or auditor visit can be limited to those services that the firm and the entities in the firm's group are using, as required by applicable legal and regulatory requirements. **Regulator access** • A regulator visit to an outsource provider's business premises can be qualified so that it only takes place if the regulator deems it necessary and required under applicable legal and regulatory requirements, but further conditions should not be applied • The outsource provider should commit to cooperate with the reasonable requests of the regulator during such a visit • 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 • There can be no restrictions regarding employees who attend from the regulator. However, regulators can and will provide relevant information about individuals who will attend. • 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.
Relationship between service providers	Outsourcing supply chains are often complex. • 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

	• The Contracts (Rights of Third Parties) Act 1999 may be relevant to these considerations • 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? Firms should consider how easily a service provider's services will interface with a firm's internal systems or other third-party systems (such as agency banking arrangements for payments).
Change management	Risks can be introduced when changes are made to processes and procedures – even where these are well established. We expect firms to have in place a comprehensive change management process, but particular note should be taken of the following points: • establishing what provision has been made for making future changes to technology service provision • establishing how the testing of changes will be carried out.
Continuity and business planning	A firm should have in place appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. Firms should: • consider the likelihood and impact of an unexpected disruption to the continuity of its operations • document its strategy for maintaining continuity of its operations, including recovery from an event, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy • regularly update and test arrangements to ensure their effectiveness • consider that disruptions could be caused by intentional cyber attacks, and that these may negate controls focused on delivering system availability (such as distribution of data to multiple locations)
Resolution (where applicable)	• Any services should be organised in such a way that they do not create additional complexity in a resolution and do not become a barrier to the resolution or orderly wind-down of a firm • For firms where stabilisation powers will, or may, be applied, this will mean that the outsourcing provider and any subcontractor should agree that neither the entry into resolution nor a subsequent change in control arising from the firm's entry into resolution shall constitute a termination event. The outsourcing provider should also agree not to delete, revoke, alter or change any data and to continue to provide services to the firm (or such other entity as necessary) for an

	appropriate transitional period following the resolution • For firms where insolvency procedures will be used, services should be set up in such a way that supports the rapid return of the firms' deposits or client assets. For example, services should be organised in such a way that would not impede the production of a Single Customer View (SCV) file in a Bank Insolvency Procedure (BIP) or the production of accurate data around client assets in a Special Administration Regime (SAR).
Exit plan	Firms need to ensure that they are able to exit outsourcing plans, should they wish to, without undue disruption to their provision of services, or their compliance with the regulatory regime. Firms should: • have exit plans and termination arrangements that are understood, documented and regularly rehearsed • know how it would transition to an alternate service provider and maintain business continuity • 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 • know how it would remove data from the service provider's systems on exit • monitor concentration risk and consider what action it would take if the outsource provider failed