The FCA focuses on the cloud with finalised guidance

The UK's Financial Conduct Authority ('FCA') has followed its 2014 guidance on general outsourcing with finalised guidance catering to outsourcing to the cloud ('Cloud Guidance'). This Cloud Guidance provides a checklist of what firms looking to move to the cloud should consider, as the prospect may make some financial services firms nervous. The Cloud Guidance is also of note to cloud providers, as it contains increased clarity in terms of what restrictions they might impose in contracts with firms, for example. Marian Ang and Dr Sam De Silva of Nabarro LLP analyse the Cloud Guidance.

Introduction

Cloud computing, or simply 'the cloud,' delivers computing resources - ranging from applications to data centres - over the internet on a pay-for-use basis. Offering cheap and flexible on-demand systems, cloud computing has seen huge uptake by companies across all industries. It is a fast-growing business: according to Gartner, the global cloud computing business will be worth $23 billion at the end of 2016, tripling to $67 billion by 2020.

It has taken some time, but finally the FCA has released the finalised version of its guidance for firms outsourcing to the cloud and other third party IT services (FG 16/5)[1] (the 'Cloud Guidance'). The Cloud Guidance is non-binding in nature and intended to help regulated firms when procuring cloud computing solutions to implement cloud services.

The Cloud Guidance follows the FCA's 2014 guidance on general outsourcing (to satisfy a section of the FCA Handbook known as SYSC 8), but the Cloud Guidance is the first time the FCA has issued guidance specifically related to cloud services.

Whilst the Cloud Guidance provides a useful checklist of issues to consider, it arguably stops short of offering comfort to firms considering whether to adopt cloud services - for example, firms may have difficulty getting a cloud provider to agree to some of the stricter physical access requirements. There are also notable gaps in the Cloud Guidance, for example advice on managing particular risks associated with different cloud service models.

The cloud

Whilst digital-centric start-ups have eagerly embraced cloud technologies, established enterprises such as those operating in financial services have faced particular challenges. Legacy systems and infrastructure cannot be easily migrated to the cloud and, together with uncertainties about the security of the cloud and lack of real-time visibility across external service providers, businesses are understandably nervous about committing to the cloud.

The FCA acknowledges the wide range of cloud services on offer: private, public or hybrid cloud, infrastructure as a service ('IaaS'), platform as a service ('PaaS') and software as a service ('SaaS'). It does not clarify particular risks associated with each model, instead acknowledging the evolving nature of cloud services and highlighting the importance of taking a proportionate and risk-based approach depending on whether the outsourcing relates to a critical or important function or is material in nature. Firms are left to decide which outsourcing option is the best fit for their business, and to identify and manage their own operational risks.

Approach

The Cloud Guidance builds on the FCA's existing approach to outsourcing. The FCA identifies three risks that are specific to cloud-based solutions over-and-above 'normal' technology outsourcing:

- customers may have less scope to request bespoke services;
- cloud providers may transfer customer data around with less visibility and control for the cloud customer; and
- cloud providers may sub-contract part of the service provided to other cloud providers, again without visibility for the customer.

One of the general principles is that regulated firms must notify the FCA when entering into, or significantly changing, material or critical outsourcing arrangements, whereby a failure of the function or services would materially impair or cast serious doubt upon the firm's ability to comply with its regulatory obligations.

The Cloud Guidance highlights that a firm must retain oversight of their cloud provider, stating that firms 'retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider.' In particular, to ensure that the firm's requirements can be complied with throughout the chain, the FCA requires a firm to identify all service providers in a supply chain involving an outsourced regulated activity.

The FCA specifies the following areas as important for firms to consider in discharging their oversight obligations:

- legal and regulatory considerations;
- risk management;

- international standards;
- oversight of the cloud provider;
- data security;
- the UK's Data Protection Act 1998 ('DPA');
- effective access to data;
- access to business premises;
- relationships between service providers;
- change management;
- continuity and business planning;
- resolution during dissolution or insolvency; and
- exit planning.

Each category is accompanied by a list of bullet points for consideration and, helpfully, the Cloud Guidance provides a number of clear statements detailing what the FCA expects in terms of certain areas.

One could disagree with the FCA's view that certain risk areas are specific to outsourcing to the cloud - because many risks and areas of interest are equally applicable to other types of outsourcing arrangement, and are issues that businesses would seek to address in any outsourcing arrangement.

We outline some of the key areas covered in the Cloud Guidance below.

Maintaining oversight of cloud provider(s)

Firms cannot delegate their regulatory responsibilities to a cloud provider, and therefore need to be clear about the scope of the service being provided and the apportioning of responsibility and accountability with the cloud provider. At a high level, the firm should allocate responsibility for day-to-day and strategic management of the cloud provider, including training staff to oversee and test the outsourced activities, to manage the risks arising and to manage an exit or transfer. Any agreement with the cloud provider should also set out suitable arrangements for dispute resolution.

Any agreement with the cloud provider should require prompt and detailed notification of breaches to the firm, and provide for their remediation

As supply chains become increasingly complex, firms should review sub-contracting arrangements to ensure that they can continue to comply with regulatory requirements. Firms should consider how service providers work together, who will take on the lead systems integration role, and how easily a provider's services will interface with their own and third party systems.

Legal and regulatory considerations

The FCA states that a firm should have "a clear and documented business case or rationale" to support the outsourcing of critical or important operational functions, and when carrying out its due diligence on the potential cloud provider must ensure that entering the outsourcing arrangement does not worsen the firm's operational risk.

In addition to reviewing the contract to ensure it is compliant with the FCA's requirements, firms must maintain an accurate record of contracts, and consider the effect of contractual governing law and jurisdiction as well as any additional legal or regulatory obligations on its arrangements with the cloud provider.

In particular, the DPA sets out eight principles and accompanying guidance which firms must meet above and beyond the Cloud Guidance. The DPA is overseen and regulated by the Information Commissioner's Office ('ICO'), which has also issued further guidance on cloud computing and on sending personal data outside the European Economic Area[2].

Firms should also take account of any external assurance, for example compliance with international standards, when conducting their due diligence on the cloud provider. Such assurance is unlikely to be sufficient on its own, but a specific audit of the service the firm is proposing to use may be useful in understanding whether the service complies with well-understood standards, and whether it is relatively stable and/or uniform across its customer base.

Access to data and business premises

Certain regulatory requirements specify that there must be effective access to data relating to outsourced activities for regulated firms, their auditors, regulators and relevant authorities[3]. Each firm should therefore ensure that any contractually-agreed restrictions on data access notifications are reasonable, and that there are no restrictions on the number of requests the firm, its auditor or regulator can put forward to access or receive data. The firm should also be ready to explain to the cloud provider that the regulator will not enter into a non-disclosure agreement with the cloud provider, but will instead treat any information disclosed as confidential, and ensure that where it cannot itself disclose data for any reason the regulator/auditor may contact the cloud provider directly.

Certain regulatory requirements will also specify that firms must have effective physical access to the business premises of the cloud provider[4]. Contractual arrangements with the cloud provider should therefore allow for:

1. Firm and auditor access - the firm can request (for itself or its auditor) an on-site visit to the relevant premises, the scope of which may be limited to the services being used by the firm, by providing reasonable prior written

notice.

2. Regulator access - the Cloud Guidance in this respect is more prescriptive. The cloud provider must allow a regulator to visit if the regulator deems it necessary and it is required under application legislation. The regulator can commit to providing reasonable notice of a visit which should take place during business hours, except in an emergency or crisis, and can commit to minimising disruption to the cloud provider's operations. However, the cloud provider must impose no restrictions regarding employees attending on behalf of the regulator (although the regulator will provide information about individuals who will attend), and must commit to cooperate with the regulator's reasonable requests during the visit.

Risk management and data security

A firm must be able to identify and manage any risks introduced by their outsourcing arrangements. The FCA requires a risk assessment to be carried out and documented, a wider consideration of industry good practices as well as the effect of different geographic locations and jurisdictions on legal and regulatory risks, and the monitoring of concentration risk (i.e. reliance on any single provider). Any agreement with the cloud provider should require prompt and detailed notification of breaches to the firm, and provide for their remediation.

As part of its security risk assessment, firms should agree (and periodically review) a data residency policy with the cloud provider, check the provider's data loss and breach notification processes, consider the segregation of data (if using a public cloud) and data sensitivity in line with how the data is to be transmitted, stored and encrypted (where necessary). The firm should take appropriate steps to mitigate security risks so that its overall security exposure remains acceptable.

Change management, business continuity and exit planning

Firms should have a comprehensive change management process in place, providing for future changes in technology service provision and establishing how changes will be tested.

In the event of an unforeseen disruption to the outsourced services, a firm should ensure that it can continue to function and meet its regulatory obligations. This requires considering the impact of a disruption, documenting a strategy for maintaining business continuity, and regularly testing (and updating) these arrangements. It also means implementing arrangements to ensure the regulator has access to data in the event of insolvency or any other business disruption.

The firm's arrangements with its cloud provider should also provide for continuity in the event of the firm's entry into resolution (and a subsequent change in control) for an appropriate transitional period. If insolvency arises, the services should be set up in a way to support the rapid return of the firm's deposits or client assets.

The FCA requires firms to ensure they have adequate, documented and tested exit plans and transition arrangements, with the cloud provider contractually obliged to assist with the transition. Firms should also plan for the removal of data from the cloud provider's systems.

Comment

Cloud computing is a fast-growing area of technology which businesses are looking for ways to integrate into their operations, including in the financial services industry. The Cloud Guidance aims to help regulated firms adopt the cloud in a safe and compliant manner that balances the risks and opportunities involved. Although quite prescriptive in certain aspects, the Cloud Guidance serves as a useful benchmark for negotiations between regulated firms and their potential cloud providers, for example, in respect of the cloud provider's positions on audit access and access by regulators. Cloud providers now have greater clarity as to the restrictions it is legitimate to impose in respect of audit.

However, it remains to be seen how willing cloud providers will be in practice to take on some of the more onerous requirements, in particular physical access requirements, and firms' inclination and actual capacity to keep such robust control of their supply chains. Hence, in some respects the Cloud Guidance could be seen as aspirational.

From the perspective of cloud providers we would hope that they see the Cloud Guidance as a clear set of requirements (albeit non-mandatory) relating to their regulated financial sector customers' compliance needs, and use it to develop contractual solutions to ensure compliance.

Marian Ang Associate
Dr Sam De Silva Partner
Nabarro LLP, London
s.desilva@nabarro.com

1. https://www.fca.org.uk/static/fca/article-type/news/fg16-5.pdf
2. https://ico.org.uk/media/fororganisations/documents/1540/cloud_computing_guidance_for_organisations.pdf, https://ico.org.uk/for-organisations/guide-toda ta-protection/principle-8-international/
3. See, for example, SYSC 8.1.8(9).
4. See, for example, SYSC 8 and Article 274 of the Solvency II Regulation.