Pinsent Masons

bba
The voice of banking

Banking on Cloud

A discussion paper by the BBA and Pinsent Masons

About the BBA Cloud Computing Working Group

In collaboration with Pinsent Masons, in early 2016 the BBA created a Cloud Computing Working Group for BBA members with the objective of identifying regulatory and commercial challenges that are holding banks back from adopting cloud solutions to a greater extent than that which to date has taken place.

This discussion paper represents the first output of the Cloud Computing Working Group and sets up a work-stream for future collaboration amongst BBA members and with stakeholders more generally, including cloud service providers. It also sets out a direction for future engagement with regulators in relation to regulatory issues which remain causes for concern for both banks and cloud service providers, while not setting out specific requests for clarification.

While this discussion paper focuses on public cloud deployment models, it is also relevant to hybrid cloud models.

Methodology

- Pinsent Masons produced an initial report and detailed roadmap agenda for the BBA Cloud Working Group to consider.
- Five BBA Cloud Working Group sessions were held where the roadmap prepared by Pinsent Masons was considered and debated.
- Requests for clarification of specific issues were made during BBA Cloud Working Group sessions and taken on by specific members.
- A questionnaire was sent out to members following on from the discussions undertaken during the BBA Cloud Working Group sessions which tested the collective view of key challenges that arose from the BBA Cloud Working Group discussions.
- Responses to the questionnaire, minutes from the BBA Cloud Working Group sessions and outputs prepared by specific BBA Cloud Working Group members were reviewed by Pinsent Masons and the BBA.
- A draft discussion paper was prepared on the basis of that review.
- Further input was sought from the BBA membership.
- Final publication took place on 5 December 2016.

Introduction

Outside of banking, public cloud computing has proven to be a driver of innovation, enabling new competitors, products and more flexible business models. By comparison, banks have been understandably slower in migrating products and services and leveraging the benefits of the public cloud, taking time first to focus on assessing risk and the necessary controls that need to be put in place. However, this trend is changing, as cloud computing is increasingly seen as a reliable, and cost-effective, opportunity and solution for banks.

One of the key drivers of this change is the digital economy. The proliferation of data and emerging demand for innovative digital products and services that meet customer needs, introduce new challenges on banks' IT infrastructure. These challenges include a pressing need to deploy cloud-enabled services and maintain capacity to process large volumes of data, combined with secure and economical storage. Many long-established, challengers and new digital banks are therefore seeking to leverage cloud in order to accelerate innovation, mitigate IT risks, and introduce cost efficiencies.

Public Cloud: Key Drivers for Adoption

1. Agile innovation

The ability to access a shared pool of configurable computing resources can increase a bank's ability to innovate by enhancing agility, efficiency, and productivity. Public cloud deployments can enable banks to direct internal resources, previously focused on the administration of IT infrastructure, towards innovating and delivering new products and services to market more quickly.

2. Risk mitigation

Public cloud can provide efficient solutions to mitigate traditional technology risks, such as capacity, redundancy, and resiliency concerns. The scalable nature of public cloud computing can provide banks with greater control in the management of variable IT demands, while offering new commercially viable methods to implement enhanced security controls.

3. Cost benefits

Cost efficiencies can be derived from reducing the initial capital expenditure investment required for traditional IT infrastructure, and through providing more efficient means for banks to manage computing capacity necessary to satisfy customer demand across peak periods. In addition to these direct cost benefits, new business efficiencies gained from public cloud deployments within bank innovation and risk mitigation processes can also deliver associated cost efficiencies.

Introduction (continued)

As banks continue to utilise cloud computing with its many new benefits to clients, customers and banks themselves, consideration needs to be given to risk mitigation and regulatory compliance issues. As part of this process, banks must identify new risks unique to the public cloud and understand how responsibility for risk controls are managed in this new environment. This includes reassessing internal controls and ensuring appropriate arrangements are in place with cloud service providers, and third parties which exercise control over aspects of the technology stack. New challenges also arise as banks apply IT and operational risk policies to technologies that challenge traditional notions in outsourcing arrangements or concerning access to, and location of, data.

That is not to suggest that banks are generally all at the beginning of this journey. Many banks are establishing well-developed positions on the challenges in which use of public cloud can result and entering into terms with public cloud service providers in relation to some functions. Others are actively working with major cloud service providers to ensure that proper controls, governance and compliance processes can be formed.

The benefits of public cloud computing are optimised for banks and their clients and customers when leveraged across jurisdictions. Internationally, regulators have acknowledged the potential of cloud computing to effect positive change in financial services. For example, the Monetary Authority of Singapore, the UK's Financial Conduct Authority (FCA) and the Australian Prudential Regulation Authority, have introduced guidance and checklists in an attempt to clarify the requirements for outsourcing to the cloud or using other third party IT services. However, inconsistent regulatory approaches across jurisdictions continue, and uncertainty around the interpretation of certain regulatory requirements remain, causing friction both within banks, and between banks and cloud service providers.

There are several steps that banks, cloud service providers and regulators can take to reduce these frictions and enable the responsible adoption of public cloud computing as part of the wider sustainable digitalisation of financial services.

Working together, banks, cloud service providers, regulators and policy makers can understand how best to meet the policy objectives of the regulatory regime while also minimising frictions to innovation and competition. There is no simple answer. However, a principle-based approach to regulation that enables banks to develop bespoke and efficient approaches to regulatory compliance and risk management is fundamental. Specific solutions should include joint industry advice on best practice, refined regulatory guidance, and risk and control frameworks to support industry benchmarking and proportionate decision making.

The way forward

Banks, cloud service providers, regulators, and policy makers should work together to:

- prioritise activities that clarify ways to meet the objectives of the regulatory regime in a public cloud computing context; and
- create a more harmonised international regulatory framework for the adoption of public cloud computing in banking.

Seven hurdles to cloud adoption

The BBA Cloud Working Group has identified a number of hurdles that impact on the extent to which banks can adopt public cloud solutions efficiently, with confidence, and without creating exposure to levels of regulatory compliance risk which they consider unacceptable.

While these hurdles exist as real and practical frictions that hold many banks back from using public cloud solutions, not all are regulatory. Many of them arise from the challenge of understanding how to meet regulatory requirements using systems, controls, processes and procedures designed for traditional outsourcing arrangements. These frictions can result in protracted negotiations of cloud contracts and also internal challenges within a bank's own risk and control function.

The seven hurdles

The hurdles are:

- difficulties in understanding whether the use of a specific public cloud technology enables a **"critical" or "important" operational function of a bank;**
- uncertainty as to what amounts to **effective supervision and oversight** of a public cloud service provider, and its supply chain;
- practical constraints in **enabling regulators to have effective oversight** of regulated activities dependent on public cloud technology;
- adapting internal risk frameworks to a new technology environment that accounts for **additional risks** that may arise in a public cloud context;
- issues concerning the **location of data** including transferring data outside the European Economic Area (EEA) and access to data by law enforcement authorities;
- issues concerning the **management of data** including security, data breach reporting and ensuring that new obligations soon to come into effect such as privacy by design and default can be effectively met in a public cloud environment; and
- difficulties in establishing a compliant **termination and exit regime** in a public cloud context.

Hurdle 1: Clarifying the context

Comments from BBA members:

"The current guidance regulates cloud technologies under the cloak of outsourcing. However, there is no direct equivalence in the equation between cloud services and outsourcing."

"Not all banking activities are critical or important in the context of regulated operations (for example customer relationship management and enterprise resource planning, or customer operations that are not time critical) and not all regulated operations may be critical or important."

"A lack of clarity for certain aspects of outsourcing guidance hampers risk assessments related to using public cloud for critical and material functions. This limits the innovation and availability of new banking services as, going forward, these can only realistically be delivered through public cloud."

"The benefits that flow from enabling a proportionate approach to criticality and importance should not be underestimated."

The hurdle

Current guidance does not enable banks to determine with certainty when the use of public cloud technology will take place within the context of a 'critical' or 'important' banking function. This uncertainty often results in a disproportionately risk-adverse approach to assessing technology risk.

Overcoming the hurdle

Banks work collectively, together with cloud service providers, to develop detailed criteria which can be used to determine with nearer-certainty whether a specific public cloud service involves a critical or important function. This output would benefit from regulatory endorsement.

The rules

If a cloud environment is used for critical or important operations linked to financial products or core activities a bank should expect that activity to be subject to stricter regulation. European legislation which applies to the outsourcing of technology and services by banks, UK secondary legislation and industry-specific guidance apply specifically to "the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services."[1]

Operational functions will be considered 'critical' or 'important' "if a defect or failure in its performance would **materially impair** the continuing **compliance**" of a bank with the "**conditions and obligations of its authorisation**"[2] or other obligations under the regulatory system, its financial performance, or the soundness or continuity of its relevant services and activities.

Examples of non-critical functions are given[3] to include advisory services and other services not regarded as core services and activities of a bank, including, amongst others, legal advice, the training of staff, billing services and the security of a bank's premises and personnel. The purchase of standardised services, such as market information services and the provision of price feeds are also listed as examples of non-critical or important services as is certain "recording and retention of relevant telephone conversations or electronic communications" required by law.

Guidance

The FCA's cloud guidance[4] refers to the general definition of a 'critical and important' function defined with reference to a defect or failure in performance which would materially impair the continuing compliance of a bank 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. It also references a 'material outsourcing' which it defines as "outsourcing services of such importance that weakness or failure of the services would cast serious doubt upon [a bank's] continuing satisfaction of the threshold conditions or compliance with the FCA's Principles for Businesses."

Beyond reference to these rules, the UK regulators have not provided any guidance which could be used to determine whether specific technology services can be considered to fall within the criteria of a critical or important operational function, or be the subject matter of a material outsourcing. In other contexts, the FCA has endorsed the views set out in MiFID Connect, an industry source of guidance, which lists the provision of the following as 'critical' or 'important':

- data storage (physical and electronic);
- ongoing, day-to-day systems maintenance/support; and
- ongoing, day-to-day software/systems management (e.g. where a third party carries out day-to-day functionality and/or runs software or processes on its own systems).

1 SYSC rule 8.1.1(1). For banks the rules on "critical and important" outsourcing in SYSC 8 are now found in the Outsourcing Part of the Prudential Regulation Authority's Rulebook. The wording of the rules in the Outsourcing Part is identical to that in SYSC 8 (and is taken directly from the Implementing Directive (2006/73/EC) of the Markets in Financial Instruments irective (MiFID) (2004/39/EC)).

2 SYSC rule 8.1.4.

3 SYSC rule 8.1.5.

4 FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf.

The hurdle in more detail

Current guidance does not enable banks to determine with certainty when the use of public cloud technology will be considered as taking place within the context of a 'critical' or 'important' banking function and therefore subject to more stringent financial outsourcing regulation. The BBA Cloud Working Group are minded that the MiFID Connect guidance conflates core operations with non-production or business-as-usual activities and is insufficient to clarify which cloud arrangements will fall within the financial regulation's outsourcing requirements and which ones will not.

As a consequence, banks often conclude that they have no option other than to decide that all or the majority of public cloud technology will be for enabling a 'critical' or 'important' function. This uncertainty prevents them from assessing technology risk in a proportionate manner and has a detrimental impact on the ability of banks to use the public cloud or leverage shared third party infrastructures to innovate and reduce cost.

The way forward

Banks work collectively and together with cloud service providers to develop criteria against which the materiality of a specific public cloud technology or service can be considered to help determine when outsourcing rules will apply. In endorsing this approach, the BBA Cloud Working Group acknowledge the work already undertaken in this regard by the Association of Banks in Singapore in its ABS Cloud Computing Implementation Guide 1.1 for the Financial Industry in Singapore published in August 2016.

Potential criteria raised by some participants in the BBA Cloud Computing Working Group for consideration include:

- the impact of the technology or service on 'critical economic functions' that the bank carries out – whether the technology or service relates to a 'core financial production activity' or conversely, an 'ordinary business activity' that can be replaced without significantly impacting regulated activities;
- the market share size and geographical coverage impacted by use of the public cloud technology or service;
- the impact of the technology or service on the bank's interconnectedness, both in terms of its ability to perform internally, and external risk factors that arise due to interconnectivity issues with external systems;
- the substitutability of the technology or service; and
- the complexity of the technology or service, in terms of supply chain, number of services, jurisdictions and other considerations.

It is important that a robust discussion is undertaken to agree common criteria to empower banks to take a proportionate approach to evaluating the relevance of individual criterion to the criticality and materiality of specific public cloud arrangements. This approach would enable banks to exercise greater flexibility in deploying technology for functions deemed not to be critical or important, opening the way for greater use of cloud solutions and innovation in areas where the more stringent outsourcing rules are deemed unnecessary.

Safeguards are currently in place that are sufficient to ensure that banks take a proportionate risk-based approach to managing risk in the context of non-critical or important functions. For one, banks are expected to observe, though in a more flexible manner, the principles behind European outsourcing rules. Further, FCA guidance on its rules provides that even where an outsourcing is not related to the performance of a critical function, a bank should take its rules into account "in a manner that is proportionate given the nature, scale and complexity of the outsourcing"[5]. Obligations to comply with data protection laws also continue to apply in a non-critical or important function context including those which relate to privacy, data security and the transfer of data to locations outside the EEA to all uses of personal data.

5 SYSC rule 8.1.3.

Hurdle 2: Ensuring effective supervision and oversight

Comments from BBA members:

"While we can outsource a capability, the responsibility for failures resides with the bank. Effective supervision is vital to manage this responsibility, in effect to act as a compensation to the fact that internal controls that are presently in force will potentially not be applied by the cloud service provider".

"Due diligence is an issue of IaaS, because on-premises infrastructure pieces usually have little to do with subcontractors."

"SaaS providers leverage multi-tenancy and other cloud service providers, 'beneath' them in the technology stack."

"Even when identification is achieved, determining the relevance to the primary service being provided in order to take a proportionate approach can also cause challenges."

"Guidance does not provide sufficient detail into which service layers, and to what level, due diligence on subcontractors is required. For instance, is it required to review the underlying data centre provider when using an IaaS service? Is due diligence required for infrastructure providers used by a SaaS provider?"

The hurdle

Banks are uncertain as to where to 'draw the line' in terms of oversight of public cloud supply chains, because of uncertain expressions set out in regulatory guidance. As a result, banks often conclude that they have no option other than to require a complete review of often complex subcontracting arrangements which may be disproportionate to the level of risk introduced by the cloud solution being procured.

Overcoming the hurdle

Support for best practice industry guidance developed by banks working collectively and together with cloud service providers, that sets out how to monitor risk across different public cloud supply chain scenarios. This would enable a more proportionate approach to risk than the view expressed in current regulatory guidance that requires banks to have oversight of all service providers in a public cloud supply chain that are 'related to the regulated activity'.

The rules

Banks are required to have internal controls in place which **achieve effective identification, monitoring and reporting** of risk.[6] Senior personnel **cannot delegate responsibility**[7] for the effectiveness of these controls and must **take steps** to demonstrate that they are **properly supervising** cloud service providers.[8]

To properly supervise a cloud service provider, a bank must **retain** the **internal expertise** necessary to demonstrate that it can effectively evaluate the cloud service provider and its performance.[9]

Guidance

The FCA's cloud guidance sets out what a bank should do 'at a high level'. Beyond restating the rules, the guidance also adds that where **"related to the regulated activity** being provided" **bank should "identify all the service providers in the supply chain** and ensure that the requirements on the bank can be complied with throughout the supply chain." A similar approach needs to be taken where there are multiple suppliers as distinct from a chain.

The guidance sets out the general principle that there should be clarity as to "where responsibility and accountability between the firm and its service provider(s) begins and ends", without providing further detail. The guidance also says that firms should "allocate responsibility for the day-to-day and strategic management of the service provider" and have "resources to oversee and test the outsourced activities."

Banks should also "review subcontracting arrangements relevant to the provision of the regulated activity to determine whether these enable the regulated firm to continue to comply with its regulatory requirements", according to the guidance.

6 SYSC rule 8.1.3.
7 SYSC rule 8.1.6(1).
8 SYSC rule 8.1.8(3).
9 SYSC rule 8.1.8(5).

The hurdle in more detail

- Effective identification, monitoring and reporting of risk is more demanding in cloud environments due to a **lack of visibility over the whole supply chain** of the technology stack. The supply chain in a public cloud environment will differ greatly depending on the model being deployed, whether infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) or software-as-a-service (SaaS) and may include a range of third parties. For example, a SaaS solution may operate on the platform of another provider, which is stored on the infrastructure of a further third provider. Given this complexity, and the propensity of cloud service providers to continually engage with different partners and providers of their own, effective identification and monitoring of risk is demanding both at the outset of a cloud contract, and during its term.
- If a bank cannot demonstrate that it has achieved effective identification, monitoring and reporting of risk, it will **fail to demonstrate that it is properly supervising** the delivery of a cloud technology or service. An inability to demonstrate visibility across a whole supply chain may also raise the issue of **whether a bank can adequately assess whether it has the internal expertise necessary** to monitor the extent to which a cloud solution impacts on the bank's compliance with the regulatory framework.
- As visibility hinges on the complexity of the supply chain – whether banks are able to determine with confidence that they have satisfied the regulatory requirement will be more difficult the more complex the supply chain and the potential number of actors involved.
- The length of cloud supply chains, and the use of multiple subcontractors to provide differing layers of a cloud service, can cause firms difficulty in ensuring that the entire supply chain agrees to adequate data security measures, particularly when the required level of data security measures are not clear or well defined.

While banks are guided to identify all service providers "where these are related to the regulated activity"[12], they are not given any clarity as to where to draw the line between a service provider in a supply chain that is relevant to the regulated activity and one that is not.

This requirement introduces a friction as it does not enable a proportionate, risk-based approach to be undertaken, and can be interpreted as requiring banks to carry out a complex review of the subcontracting arrangements which is disproportionate to the level of risk introduced by the cloud solution being procured. This is detrimental to banks looking to innovate and to consistently apply a proportionate approach to risk.

The way forward

- Banks work collectively, and together with cloud service providers, to develop best practice guidance which provides clarity on how firms can take a proportionate approach to ensure the effective identification and monitoring of risk, throughout the supply chain.
- Cloud service providers and banks should seek to create a standardised approach to the disclosure of information, in relation to the provider's supply chain, relevant to the bank's regulatory obligations, and focusing on specific scenarios and use cases.

10 FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf, page 6.
11 FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf, page 10.

Hurdle 3: Regulatory oversight – ensuring regulators have the access they require to effectively regulate banks

Comments from BBA members:

"From a practical perspective, allowance for remote access for audit purposes could help firms negotiate more frequent access improving their ability for on-going monitoring."

"Audit rights of SaaS provider[s] are often not critical or helpful. Audit rights of the underlying IaaS provider are more important [but] unobtainable because the SaaS provider cannot offer or contract for rights it does not have."

"The infrastructure layer of modern cloud is highly virtualised and distributed; on-site auditing has little effectiveness: access should preferably be expressed as logical, more than physical, to be more effective."

"As in the cloud and IT networks in general, data can be anywhere and everywhere. However, if the data can be accessed only by residents (and regulators) of a country, then data segregation (by tokenisation or encryption) can provide meaningful access for audits."

"Where the infrastructure layer of cloud is shared by multiple tenants, on-site auditing of such premises by one tenant might increase the operational risk of other tenants."

"Configuration and management systems are fully available remotely so there is no advantage to being at the physical site except to evidence things related to physical lifecycle of equipment."

"Regulator (or enforcement authority) action can also have a negative effect in the sector during 'dawn raid' investigations, where data from various banks is likely to be hosted in the same shared facilities. As an example, impounding a server stack will disrupt other tenants hosted in that facility."

"Some regulatory activity is seen differently by industry and its customers. On the one hand, there are authorities which elicit public trust: as they make banking safer, or protect the public from unauthorised data uses, and which investigate individuals and companies to ensure banks are not involved in criminal activities; and on the other hand, there are agencies that operate with little transparency and with uncertain remit or geographical limits and which elicit public suspicion. Data access to the latter category is often seen as problematic by regulators".

The hurdle

*Banks are unclear about the extent to which they can **limit the rights of regulators to access business premises** from which public cloud services are provided despite a recent attempted clarification in FCA guidance. This can result in protracted contractual negotiations between banks and cloud service providers.*

Overcoming the hurdle

*Regulators should endorse an approach that recognises that physical access to public cloud data centre premises need only be provided **as a final measure** where effective access cannot be enabled by remote means.*

The rules

When entering into a cloud arrangement, banks must ensure that the arrangement does not **impair materially** a **regulator's ability to monitor** a bank's compliance with its regulatory obligations.[12] This requires banks to take steps to demonstrate that a regulator can exercise a right of effective access to data relating to the arrangement.[13] The bank must also take steps to demonstrate that a regulator can exercise a **right of effective access to the business premises** of service providers processing that data.[14]

More broadly, banks must demonstrate that they are using service providers that commit to **co-operating with regulators** in connection with oversight of the cloud arrangement.[15]

Guidance

The FCA's cloud guidance states that: "A firm should be able to request an on-site visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. **This right should not be restricted**".

It also states that: "We agree that **physical access to data centres may not always be necessary** to provide effective access, **but** we also consider that **there may be circumstances where physical access to data centres is necessary** for a firm to meet its regulatory requirements" and that "The focus should … 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**."

12 SYSC rule 8.1.1(2).
13 SYSC rule 8.1.8(9).
14 SYSC rule 8.1.8(9).
15 SYSC rule 8.1.8(8).

The hurdle in more detail

- There is uncertainty as to the scope of the rights of access to both data and premises required by regulators that must be negotiated in contractual arrangements in order to satisfy these regulatory requirements. The FCA's cloud guidance does little to remove uncertainties as to the scope of audit rights that are required to be secured from cloud service providers. As a result, banks and cloud service providers must enter into protracted negotiations which introduce inefficiencies, increasing costs and time associated with public cloud deployments.
- The BBA Cloud Working Group note that cloud service providers are generally not prepared to agree to audit rights which require them to provide on-site access to their data centres and other premises. This can be due to a number of reasons, but commonly because the cloud service provider is providing a global, commoditised, multi-tenancy service and audit rights of this nature create friction with that business model.
- The BBA Cloud Working Group also agree that even if on-site access to cloud service provider premises can successfully be negotiated, there do not appear to be real and compelling advantages in accessing physical infrastructure as compared to logical access to bank data in a virtualised environment.

More generally, there is a tension between emerging technologies of a distributed nature such as cloud computing and traditional approaches to regulatory supervision of outsourcing to third party suppliers. In a cloud structure where data is moved, shared, supported and replicated across different data centres and geographies, it is important to make clear the policy objectives sought to be achieved through traditional approaches to regulatory oversight, and how they can be achieved most effectively given rapid developments in technology and business models. For example, logical (rather than physical) access to data may be a more effective mechanism for enabling effective regulatory oversight.

The way forward

Banks work collectively and together with cloud service providers to clearly define objectives and expectations regarding regulatory oversight, and how best they can be achieved in a public cloud context. A number of considerations will need to be addressed, including the following:

- clarity around when business premises will be 'relevant for the exercise of effective oversight';
- specifying the types of circumstances where physical access may be necessary for a bank to meet its regulatory requirements;
- clarity as to how to reconcile the guidance that a bank should be able to 'request an on-site visit to business premises' that 'should not be restricted' with a service provider's right to 'limit access to some sites – such as data centres' in contractual terms. For example, can parties reach an agreement that certain data centre premises can never be physically accessed for security reasons so long as effective oversight is achieved by other means?; and
- recognition of the need for continued discussion as to how independent third party audit regimes can be effectively used beyond assessing data security.

Generally, regulators should specify more directly the categories, purposes and level of detail of information required to achieve regulatory oversight objectives.

Hurdle 4: Additional risks – addressing distinct cloud risks

Comments from BBA members:

"Both banks and regulators would benefit from collaboration and knowledge sharing when it comes to identifying and mitigating new risks arising from public cloud computing."

"The more of the overall technology stack provided by the vendor, the more important it becomes to understand what is truly going on under the hood."

The hurdle

Public cloud services introduce different or additional operational risks that do not arise in non-public cloud environments. This creates new challenges for banks in ensuring compliance with internal risk profiles and policies, and can lead to protracted contractual negotiations. If not adequately addressed, this can also result in regulatory non-compliance.

Overcoming the hurdle

Banks work collectively and together with cloud service providers to develop endorsed industry standards setting out the steps to be taken to address operational risks that arise in a public cloud context.

The rules

Banks must not take on any **undue additional** operational risks when entering into an outsourcing arrangement, and must **take steps** to avoid undue additional operational risks arising.[16]

Guidance

'Operational risk' is not defined in the context of UK and EU financial services outsourcing rules. However, a general common definition which arises out of the work undertaken by the Basel Committee on Banking Supervision is applied across a number of banking contexts. That definition generally equates operational risk to the potential impact of losses stemming from inadequate or failed internal processes, people and systems or from external events. It includes legal risk but excludes reputational risk.

The FCA's cloud guidance does not comment on the definition of operational risk. Confirmation that the regulator is assuming that the general definition applied to operational risk by the Basel Committee and subsequently set out in the EU Capital Requirements Regulation (CRR)[17] is applicable to the context of outsourcing generally, and cloud procurement specifically, would add certainty for banks in addressing compliance with this rule. The BBA Cloud Working Group is of the view that the concept of what is 'operational' should be linked to financial products and core activities, and the significance of this risk should be granularised.

Further, the European Banking Authority (EBA) recently published a consultation paper on draft guidelines relating to how national regulators across the EU should assess information and communication technology (ICT) risk for the purposes of the supervisory requirements under the package of measures known as the Capital Requirements Directive IV (CRD IV) (including the Capital Requirements Regulation). Specifically, they provide "a supervisory methodology for the assessment of ICT risk as part of Operational Risk under…the CRD"[18].

Though the guidelines are currently only in draft form and are aimed at national regulators rather than banks, they do provide additional clarity on the types of risks which the UK authorities will be required to supervise in relation to ICT in banks. In particular, an annex to the draft guidelines sets out a non-exhaustive list of ICT risks which the EBA considers to have a potentially high severity or operational, reputational or financial impact on banks. The guidelines also set out various definitions, including one for "ICT outsourcing risk" which is "the risk that engaging a third party... to provide ICT systems or related services adversely impacts the [bank's] performance and risk management".

The FCA's guidance does not directly identify **criteria to assess when an operational risk in a public cloud is an 'undue risk'.** Additional granularity in respect of multi-tenancy and shared platforms' distinct risks is also needed to assist complying with this requirement.

The FCA's guidance clarifies however, that banks cannot argue that although an arrangement may worsen overall operational risk, it would still fit within the firm's risk appetite and therefore will not introduce an 'undue additional risk'. The FCA's position is that if a cloud arrangement worsens operational risk, then a bank cannot enter into it. According to the FCA's cloud guidance the practical steps to be taken to avoid undue additional operational risks include:

- carrying out a risk assessment to identify relevant risks;
- documenting that assessment; and
- identifying current industry good practice that could be used to support decision making.

16 SYSC rule 8.1.1(1).
17 As defined in Article 4(1)(52) of the CRR (Regulation EU 575/2013).
18 Consultation Paper EBA/CP/2016/14, dated 6 October 2016, page 6.

The hurdle in more detail

- There is increasing pressure on banks to interpret a growing number of changes in law and regulation correctly and respond with effective risk identification and management processes, and ensure that these processes are not weakened through third party supplier relationships. Regulators will hold banks accountable for failures they consider significant and which could lead to financial stability risks and interference with other key regulatory policy objectives, whether those failures relate to capital assessments, stress testing or identifying and managing existing and emerging third party supplier risks.
- The FCA has demonstrated its willingness to respond to failures to manage new and emerging risks, for example with issues arising out of Payment Protection Insurance schemes (PPI). A bank therefore that does not respond, or responds slowly to the identification of an emerging risk leaves itself exposed to regulatory enforcement.
- The challenge for banks is to **ensure that risk methodologies are robust to deal with new risks in the public cloud.** Whether a bank relies on annual emerging risk assessments, quarterly reports, scenario planning exercises, risk committee procedures, analysis of third party data or other processes in managing risk, regulators expect that adequate attention and investment will be given to specific areas of concern.
- New operational risks arise from public cloud technologies and services, and existing risk models must be adapted to take account of these risks. Without the regulator helping the industry model and validate how to identify and manage public cloud specific risks, an uneven approach to risk management will continue amongst banks, harming or delaying the adoption of public cloud technologies.
- The BBA Cloud Working Group is minded that the current uncertainty in public cloud regulation leads to banks diverting resources in risk management towards regulatory compliance and to increased time and resource required to negotiate cloud agreements, and increasingly for some banks, to a proportion of those negotiations being suspended, reduced in its UK scope or abandoned.

The way forward

Banks should work collectively and together with cloud service providers to share knowledge and develop industry standards setting out criteria for determining whether specific operational risks that arise when a public cloud arrangement is entered into are 'undue' or not. This exercise may require:

- identifying all significant risks that could arise in the context of a cloud arrangement that would not arise if the same service or function were performed in-house, and how to demonstrate that reasonable efforts have been undertaken to mitigate these risks;
- identifying which of these risks are 'undue', in the sense that they are excessive or disproportionate to the benefits that the arrangement creates for the bank and its customers or any means by which they can be effectively mitigated; and
- identifying ways to mitigate additional risks in a way that will render them below the threshold of 'undue operational risks' and accordingly not hurdles to enter into a specific cloud arrangement. This would include ensuring that binding commitments are obtained from the cloud service provider to this effect.

Hurdle 5: the location of data

Comments from BBA members:

"Global banks have great difficulty in nuancing their approach to data localisation across different regions."

"Cloud services are virtual and global by design. There is a risk that limiting that design by requiring regional or country solutions may reduce the security and robustness of the service."

"The growth in data locality requirements by national regulators increases cost and restricts services that can be provided effectively to customers globally. There is an opportunity to provide a more forward looking regulatory approach, focusing on controls such as encryption at rest and ensuring regulator access to data, rather than requiring data stay within a certain jurisdictional boundary."

"Regulators and policy makers should consider how to enable new technological solutions to provide alternative methods to achieve policy objectives."

The hurdle

Increasing data localisation requirements, uncertainty as to the long term validity of current mechanisms available for transferring data outside national and regional borders, and the threat of access by law enforcement authorities make it difficult to take an internationally consistent approach to technology risk management. Particularly for global banks, this increases uncertainty and introduces additional business inefficiencies and costs when seeking to leverage public cloud services, and manage the ongoing relationship.

Overcoming the hurdle

Renewed advocacy at international level for a consistent approach to be taken to the regulation of cross-border transfers of data should take place.

The rules

Other than enabling effective access by regulators to business premises of cloud service providers, neither EU nor UK financial regulation requires banks to keep data within specific locations. **Data protection laws** on the other hand **require that steps be taken if 'personal data' is to be processed at locations outside the EEA**[19]. Many countries have adopted data protection laws with data transfer restrictions meaning that banks operating globally are facing the challenge of complying with multiple (but not necessarily similar) data protection regimes when using a public cloud service provider and the landscape of cross-border data transfers is changing rapidly.

Perhaps the most common way for banks to comply with data transfer rules is for a bank and cloud service provider (or one of its subcontractors, depending on the structure of the arrangement) to enter into **standard contractual clauses** (known as the 'model clauses'), which have been pre-approved by the European Commission. Adopting these clauses enables transfers of personal data to be made outside the EEA in compliance with the data transfer rules.

Other ways include: (i) processing data on premises located in a country that the European Commission has designated as an approved 3rd country for data protection purposes; (ii) obtaining approval by data protection regulators of internal rules to govern the transfer of data, known as binding corporate rules; and (iii) in respect of transfers to the United States – registration on the EU US Privacy Shield which enables US cloud service providers to self-certify adequacy of their data protection arrangements. It is also possible for a bank to conduct an internal assessment of the adequacy of the locations at which data will be processed in accordance with guidance provided by the Information Commissioner's Office (ICO).

Guidance

The FCA's guidance states that banks should "agree a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed." It also says that "This policy should be reviewed periodically."

Guidance from the ICO highlights that where model clauses are used, they cannot be amended and must be adopted in their entirety.[20]

While the BBA Cloud Working Group recognises the benefits of agreeing a data residency policy with cloud service providers, the Group highlights that the fundamental issue is the standards of governance and protection of data, not its physical location. Further, regionalisation strategies are difficult for global banks to implement, due to inconsistencies of requirements across jurisdictions. The BBA Cloud Working Group notes that many cloud service providers, especially the larger providers, are reluctant or unwilling to accept a data residency policy that requires them to obtain consent from a bank before changing the cloud service provider's processing locations.

The BBA Cloud Working Group also observes that there is an increasing encroachment of legislation and regulatory demands for data residency in China, Luxembourg, Tanzania, Russia, Uganda, South Korea, and other countries, where such a residency policy can be seen more as a hindrance than as an enabler.

19 Eighth data protection principle of the Data Protection Act 1998, and Chapter V of the General Data Protection Regulation (EU 2016/679) (to apply from 25 May 2018).
20 ICO, The Guide to Data Protection: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-6.pdf, page 92.

The hurdle in more detail

- Cloud supply chains make it difficult to determine where data is being processed and stored because cloud service providers may not be transparent about the countries where they process data (in order to retain operational and commercial flexibility). A public cloud offering can make this determination impossible if copies of fragmented data are processed in multiple countries simultaneously to enhance data security, disaster recovery and resiliency. This makes it difficult for banks to understand what mechanisms should be put in place to comply with their data transfer obligations since that will often depend on understanding (i) all of the contractors in the supply chain, and (ii) the locations at which any 'personal data' is processed.
- The commercial operating model of most public clouds means that many cloud service providers insist on retaining full discretion to change the way that they process personal data, including the country locations of their processing and the identity and location of subcontractors they engage to conduct the processing. Some public cloud service providers recognise this issue and offer to keep personal data within defined regions, although these regions often do not match the jurisdictions in which the banks operate.
- Not all cloud service providers understand that standard contractual clauses must be agreed without amendment or 'hybridisation' with their own standard contracts. In the UK context, any amendments to those clauses would risk invalidating them according to the ICO, bringing a risk of investigation and enforcement action.
- Regulators in different EU jurisdictions have different approaches towards data transfers in the sense that they may insist on approving transfers prior to them taking place, which does not promote the speedy implementation of global cloud solutions.
- Cloud service providers may be subject to regimes in the countries they operate that require them to make data available to law enforcement agencies. Where cloud service providers process a bank's data in countries where regimes of this nature apply then that data may be subject to disclosure to authorities operating in those countries, which presents reputational risks to the bank (particularly if the data consists of information relating to its customers) and data protection regulatory non-compliance consequences in other jurisdictions. The lack of visibility of, and control over, the cloud supply chain, as well as the locations of data processing, mean that banks may become exposed to risks of this nature before they are able to take measures to prevent cloud service providers disclosing their data.

The way forward

- Banks, cloud service providers, regulators and policy makers should engage in advocacy at international level, supporting a consistent approach to be taken to the regulation of cross-border transfers of data.

- The BBA Cloud Working Group is of the view that the FCA should clarify in its guidance that 'agreeing a residency policy' should only be done when this is necessary to ensure compliance with an existing legal or regulatory requirement for data localisation, rather than as standard practice.

Hurdle 6: management of data (including data breach reporting)

Comments from BBA Members:

"Currently, reporting data breaches to the ICO is considered good practice. Looking forward, several developments are likely to increase the amount of reporting required and make much of it mandatory (GDPR, NIS and PSD2), compounding existing issues."

"Different regulators have varying requirements around security breaches; from a contractual perspective this can prove very difficult to negotiate and if not able to meet may mean that we are unable to rollout in that particular jurisdiction."

"The most noticeable area of reporting is the inconsistency between the FCA and ICO. Reporting the same issue to two separate authorities is inefficient but also time-consuming when they don't ask for the same type and level of information."

"Often the assessment of the impact of a data breach or cyber incident involves detailed investigations, which may take time. Notification within an unrealistic time frame is likely to mean that the scope of the incident is not fully understood and will inundate the regulators with information that does not accurately reflect the extent of the potential or actual risks."

The hurdle

A lack of transparency as to the structure and management of data governance arrangements in a public cloud environment creates friction, particularly in relation to the frequency and format of meetings and the content of data breach reporting obligations. How new obligations created by the General Data Protection Regulation (GDPR) are to be met in a public cloud environment must also be clarified.

Overcoming the hurdle

Banks should work collectively and together with cloud service providers to develop a standardised approach to the mapping of cloud contractual provisions and public cloud service provider processes against data management requirements endorsed by the regulator.

The rules

Banks are required to ensure that use of a cloud solution **does not impair materially** the **quality of its internal controls**.[21] Both existing data protection rules and those that will take effect under the GDPR require banks to demonstrate that they have adequate data security measures in place,[22] while data breach reporting regimes are spread across a number of different legal instruments.

A bank must ensure that any cloud arrangement does **not undermine or alter in a negative way a bank's relationship and obligations towards its clients**.[23] Clients of banks have privacy-related rights in respect of personal data, including rights to access personal data, have personal data rectified where inaccurate, have personal data erased (or 'forgotten') and, once the GDPR comes into force, to ensure that personal data can be made 'portable' and transferred from one institution to another.[24]

The GDPR lists in **general what is expected in terms of achieving adequate security**[25] to include the use of pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. It also provides that **adherence to an approved code of conduct** or an **approved certification mechanism** may be used as an element by which to demonstrate compliance.

In terms of incident reporting, there are overlapping requirements:

- Financial regulation requires banks to **notify the regulator immediately**[26] on becoming aware or having information which suggests that a matter which could have a **significant adverse impact** on the firm's reputation has occurred or is likely to occur in the foreseeable future. Banks must also notify the regulator where a matter could **affect the firm's ability to continue to provide adequate services** to its customers that could result in **serious detriment to a customer** or have **serious financial consequences** to the UK financial system or to another financial institution.[27]

- The GDPR will require banks "without undue delay and, where feasible, **not later than 72 hours** after having become aware of it" to notify personal **data breaches** to data protection authorities unless the breach is unlikely to "result in a risk to the rights and freedoms of natural persons"[28]. The notification must describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, describe the likely consequences of the personal data breach and the measures taken or proposed to be taken to address the incident.

- The Network and Security Directive will similarly impose **notification obligations** on banks in respect of a broader category of 'security incidents' defined to include ' any event having an actual adverse **effect on the security of network and information systems**'[29].

- The GDPR will also introduce a number of further **new operational requirements** including an obligation on banks to implement appropriate technical and organisational measures for **ensuring that, by default, only personal data which are necessary for each specific purpose of processing are processed**.[30]

Guidance

The FCA's cloud guidance contains general guidelines to help banks ensure that their use of a cloud solution does not impair the quality of its internal controls. The guidance indicates that firms should ensure that they **appropriately identify and manage the operational risks associated with the use of third parties, including carrying out due diligence** before using a cloud service provider.

This guidance does not, however, directly address or specify how banks can ensure that their cloud service providers have adequate data security measures in place, nor does it provide useful guidance on ensuring compliance with data breach notification requirements. The guidance instead refers to ICO guidance in relation to these matters.

The ICO[31] does provide cloud-specific guidance on how firms can ensure adequate data security measures are in place and encourages firms to **assess data protection risks, to carefully select their cloud service provider and to ensure they have suitable contracts with cloud service providers that allow them to continue to monitor performance**. The ICO guidance does not address in any detail when a firm would be obliged to notify a data breach to the ICO and does not contain cloud specific guidelines on how to do so effectively.

The hurdle in more detail

The potential for a lack of consistency from regulators about when data breaches should be reported, what information needs to be provided when they are reported and the timescales in which they must be reported make cloud adoption more difficult for banks, adding unnecessary administrative burden and cost. This issue would be exacerbated if regulatory guidance were to take the view that data breaches should be reported at too early a point when it may not be possible to adequately assess the detail and causes of the incident.

We understand the ICO is currently preparing to provide further specific cloud guidance that addresses data management issues including the updated requirements under new data protection laws regarding data protection 'by design and default' and data breach notification. This guidance should ideally build on the current general cloud guidance that is available and give firms specific requirements and timescales that can be addressed when negotiating with cloud service providers.

The way forward

- Industry collaboration to ensure that data breach notification requirements are, as far as possible, implemented in a consistent manner across regulators to reduce duplication of effort and cost to firms when notifying data breaches both domestically and internationally should be prepared. Banks should be able to make a data breach notification in one place, rather than notifying each regulator separately. Banks will also benefit from specific requirements about how material a data breach must be before it must be reported to a regulator.

- Cloud service providers should provide further assurance to banks by being transparent about the means by which customers of banks can exercise their privacy related rights.

- Banks work collectively and together with cloud service providers to agree a common standard of notification of data breaches to banks that is regulator-endorsed, so that there is standardisation in the way in which breaches are reported from provider, to bank, to regulator.

21 SYSC rule 8.1.1(2)(a).
22 Seventh data protection principle of the Data Protection Act 1998, and Article 32 of the GDPR.
23 SYSC rule 8.1.6(2).
24 Section 3 of the GDPR.
25 Article 32 of the GDPR.
26 FCA SUP 15.3.1.
27 FCA SUP 15.3.1.
28 Article 33 of the GDPR.
29 Article 4(7) of NIS 2016/1148.
30 Article 25 of the GDPR.
31 ICO, Guidance on the Use of Cloud Computing: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf.

Hurdle 7: Termination and exit

BBA Member comments:

"The ability and cost to effect an exit by recreating cloud services of any type, within other clouds, is high."

"Ensuring that the firm has local copies of critical data in an on-premises backup capacity is also very important."

"We need to be clear when considering termination if the termination is a particular partner relationship or if it's a termination of the use of cloud generally. The former is obviously more useful."

"A guide as to acceptable criteria for cloud transition services would be very helpful.''

"There needs to be guidance on what 'fully tested' means in relation to exit plans in a cloud context."

The hurdle

Terminating and exiting a public cloud arrangement presents an unknown challenge. This uncertainty presents challenges for banks internally in understanding how to manage risks that arise from transitioning technology and satisfactorily meeting regulatory expectations in the context of using a third party public cloud service provider.

Overcoming the hurdle

Greater transparency as to the regulator's expectations of the detail behind steps to be taken when transitioning from a public cloud environment is needed.

The rules

Banks must take steps to ensure that they exercise **due skill, care and diligence when terminating** a cloud arrangement.[32] The content that sits behind this principle is set out across a number of other regulatory rules, but the fundamental outcome must be that termination and exit arrangements enable a bank to continue to function "**without detriment to the continuity and quality**" of its services to its clients.

Guidance

According to the FCA's guidance banks need to ensure that they can exit cloud arrangements "**without undue disruption** to their provision of services, or their compliance with the regulatory regime."

The guidance outlines three key elements of an effective exit strategy. First, banks must ensure that their exit plans and termination arrangements are **documented** and understood by appropriate staff. This documentation must include a specific contractual obligation which provides that the cloud service provider will "**cooperate fully** with **both the firm and any new outsource provider(s)** to ensure there is a smooth transition."

Second, the arrangements must also be "**fully tested**." The FCA has confirmed that this does not require banks to ensure that their exit plans are "regularly rehearsed."

Third, a bank must "**monitor concentration risk** and consider what action it would take" if its cloud service provider were to fail. The FCA has confirmed that 'concentration risk' relates to the reliance that a bank itself may have on any single provider rather than the risk of many firms using the same provider.

As well as these elements, a bank must "**know how it would transition to an alternative service provider and maintain business continuity**" including "how it would **remove data**" from the cloud service provider's systems.

The hurdle in more detail

- The operational challenges in taking on a large scale technology change programme cannot be underestimated. A failure to manage the transition of critical IT infrastructure could result in financial and reputational losses and, as has been seen in the recent past[33], capital shortfalls from which it can take a bank many years to recover.
- More certainty is therefore needed as to **the detail of the steps required** to be taken by banks and the commitments to be obtained from cloud service providers in respect of termination and exit in order to assist banks achieving the level of comfort needed to make decisions to invest in innovative and cost efficient technology solutions.

32 SYSC rule 8.1.7.
33 See, for example: Sir Christopher Kelly, Failings in management and governance: Report of the independent review into the events leading to the Co-operative Bank's capital shortfall: http://www.coop.co.uk/PageFiles/989442031/kelly-review.pdf.

The way forward

Whether in a public cloud environment or not, transitioning from one technology service to another will be a highly complex operation where critical functions of a bank are involved. All banks, service providers and regulators recognise the need for transitional arrangements to be carefully documented and meaningfully tested.

As no bank has ever exited from a significant public cloud technology arrangement, there is limited industry experience to learn from, and as a result frictions arise as to the contractual terms between banks and cloud service providers and other third parties leveraging public cloud. While these frictions may not seem distinct in and of themselves from those that present in a non-public cloud environment, there is added pressure as parties do not have the benefit of experience to call upon.

Accordingly, the BBA Cloud Working Group is of the view that the FCA should work with industry to produce a best practice due diligence checklist for banks considering migration from public cloud environments. The BBA Cloud Working Group believes that the checklist should enable banks to assess public cloud environments against criteria developed for each of the suggested headings shown here:

- expectations as to when 'termination assistance' commences and ends;
- transparency around technical issues that could cause a service failure or other unplanned disruption that would not arise in a non-public cloud environment;
- expectations around the level of information to be provided back to banks from cloud service providers to enable re-tendering for the service, as well as the level of co-operation expected as between cloud service providers in facilitating the transfer of services from an incumbent to a replacement cloud service provider;
- expectations as to duties of personnel to be involved in providing transitional services including the role of senior management;
- expectations as to data recoverability in terms of technical matters, such as formats, and commercial ones, such as timing;
- credentials and certifications in regards to security and data protection that should be provided;
- service performance and usability details;
- data location details;
- portability and recovery arrangements; and
- business continuity arrangements.

The BBA Cloud Working Group proposes that compliance with an FCA-approved checklist of this nature would go some way to demonstrating that the bank has taken steps to ensure that it has exercised due skill, care and diligence before entering into a cloud arrangement.

Contacts

Luke Scanlon
Head of Fintech Propositions
Pinsent Masons
T: +44 (0)20 7490 6567
E: luke.scanlon@pinsentmasons.com

Matthew Herbert
Director, Strategy and Digital
BBA
M: +44 (0)7712 389322
E: matthew.herbert@bba.org.uk

Craig Callery
Associate
Pinsent Masons
T: +44 (0)131 225 0078
M: +44 (0)7468 715947
E: craig.callery@pinsentmasons.com

Matthew Field
Policy Adviser, Digital
BBA
T: +44 (0)20 7216 8922
M: +44 (0)7725 350263
E: matthew.field@bba.org.uk

Yvonne Dunn
Partner, TMT
Pinsent Masons
T: +44 (0)141 249 5460
E: yvonne.dunn@pinsentmasons.com

Ronald Kent
Managing Director
BBA
T: +44 (0)20 7216 8841
M: +44 (0)7771 922052
E: ronald.kent@bba.org.uk

Our offices worldwide

London
30 Crown Place (Headquarters)
Earl Street
London
EC2A 4ES
UK
T: +44 (0)20 7418 7000
F: +44 (0)20 7418 7050

Aberdeen
13 Queen's Road
Aberdeen
AB15 4YL
UK
T: +44 (0)1224 377 900
F: +44 (0)1224 377 901

Beijing
10th Floor
Beijing China Resources Building
No 8 Jianguo Menbei Avenue
Beijing 100005
PRC
T: +86 10 8519 0011
F: +86 10 8519 0022

Belfast
The Soloist Building
1 Lanyon Place
Belfast
BT1 3LP
UK
T: +44 (0)28 9089 4800
F: +44 (0)28 9089 4801

Birmingham
3 Colmore Circus
Birmingham
B4 6BH
UK
T: +44 (0)121 200 1050
F: +44 (0)121 626 1040

Brussels*
Office 15
4 rue de la Presse
1000 Brussels
Belgium
T: +44 20 7418 7000
F: +44 20 7418 7050

Doha
PO Box 22758
Tornado Tower
West Bay
Doha
State of Qatar
T: +974 4426 9200
F: +974 4426 9201

Dubai
The Offices 1
One Central
PO Box 115580
Dubai
United Arab Emirates
T: +971 (0)4373 9700
F: +971 (0)4373 9701

Düsseldorf
Wilhelm-Marx-Haus
Heinrich-Heine-Allee 53
40213 Düsseldorf
Germany
T: +49 (0)211 88271 500
F: +49 (0)211 88271 501

Edinburgh
Princes Exchange
1 Earl Grey Street
Edinburgh
EH3 9AQ
UK
T: +44 (0)131 777 7000
F: +44 (0)131 777 7003

Third Floor Quay 2
139 Fountainbridge
Edinburgh
EH3 9QG
UK
T: +44 (0)131 225 0000
F: +44 (0)131 225 0099

Falkland Islands
56 John Street
PO Box 21
Stanley
Falkland Islands
T: +500 22690
F: +500 22689

Glasgow
141 Bothwell Street
Glasgow
G2 7EQ
UK
T: +44 (0)141 567 8400
F: +44 (0)141 567 8401

123 St Vincent Street
Glasgow
G2 5EA
UK
T: +44 (0)141 248 4858
F: +44 (0)141 248 6655

Hong Kong
50th Floor
Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
T: +852 2521 5621
F: +852 2845 2956

Istanbul
Büyükdere Caddesi No 127,
Astoria B Kule,
Kat 5, No 13-14-15-16
Esentepe 34394 Şişli
Istanbul
Turkey
T: +90 212 336 6050
F: +90 212 336 6051

Leeds
1 Park Row
Leeds
LS1 5AB
UK
T: +44 (0)113 244 5000
F: +44 (0)113 244 8000

Manchester
3 Hardman Street
Manchester
M3 3AU
UK
T: +44 (0)161 234 8234
F: +44 (0)161 234 8235

Melbourne
Level 23
360 Collins Street
Melbourne
VIC 3000
Australia
T: +61 3 9909 2500
F: +61 3 9909 2501

Munich
Ottostrasse 21
80333 Munich
Germany
T: +49 (0)89 203043 500
F: +49 (0)89 203043 501

Paris
21 – 23, Rue Balzac
75406 Paris CEDEX 08
France
T: +33 1 53 53 02 80
F: +33 1 53 53 02 81

Shanghai
Room 4605
Park Place
1601 Nanjing West Road
Shanghai 200040
PRC
T: +8621 6321 1166
F: +8621 6329 2696

Singapore
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)65 343 412

Sydney
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801

Correct as of 4 July 2016. *Representative office

www.pinsentmasons.com/fintech