INSTITUTE of INTERNATIONAL FINANCE

October 2018

CLOUD COMPUTING IN THE FINANCIAL SECTOR

PART 2: BARRIERS TO ADOPTION

1. INTRODUCTION

While data is a key asset for the digital economy for all sectors, it has always been at the core of the financial services industry. Being able to make the most of data is a central determinant not only for which firms will thrive as market leaders, but also in their ability to keep pace and survive.

Cloud computing is a key enabler in management of the large datasets commonplace in financial services, and it presents numerous benefits and opportunities in meeting evolving customer expectations. With greater customer demands for immediacy and personalization, as well as the increasing technical risk and cost associated with maintaining legacy IT infrastructure, the business case for adopting cloud technology is increasingly compelling, and the prevailing questions are less about "if," and more about "how."[1]

Amongst regulators and FIs alike, any migration to cloud is firstly underpinned by a thorough risk assessment, considering the risks and benefits as described in our Part 1 paper. However, even once those risks are managed, there remains a number of additional barriers to adoption of this technology.

For institutions that have decided that cloud will be part of their strategy, there can still be some considerable constraints caused by regulation, both specific to financial services, as well as regulation and legislation targeting data privacy and security. Together with international inconsistencies and variances in interpretation and enforcement, these add to the costs of deploying cloud computing, and they erode the business case for doing so.

Additionally, the use of cloud computing by regulated FIs is still relatively new. There are steps that should be taken by the industry, in cooperation with Cloud Service Providers (CSPs) and regulators, to ensure that cloud computing can be used efficiently, safely and securely in financial services. In this context, it is acknowledged that there are barriers that are not regulatory in nature, and relate more to organizational preparedness for cloud migration (described further in Box 2).

Such underlines that the challenge to realize cloud's benefits and risk mitigants is a shared task for FIs and their supervisors alike. As well as the commercial and strategic benefits for firms, cloud is critical for regulators keen to ensure operational resilience, digital innovation and the secure use of data.

Accordingly, this paper, the second in a 3-part series on cloud technology in the financial services industry, examines the practical hurdles in migrating to cloud, where these arise from regulation and other sources, and what steps the industry and regulators should consider taking to address these concerns. Remaining concerns related to the nature of the cloud computing market, closely connected to the CSPs, which will be addressed in the third paper in this series.

---

[1] A detailed analysis on cloud computing definitions, benefits, risks and mitigants is set out in our Part 1 paper, at: https://www.iif.com/publication/regulatory-comment-letter/iif-cloud-computing-paper-part-1

Box 1: Cloud Benefits and Risks

As with any new technology, cloud invariably has risks. Part 1 of this series identified the risks and the commensurate benefits of cloud computing, acknowledging that these could only be realized if correct due diligence and risk assessment were conducted, and the migration to cloud is done in a secure manner. The paper also identified that the biggest risk related to cloud computing may in fact be the risk of not moving to cloud.

Financial institutions that do not pursue cloud technology will not only carry a greater technical risk from the need to support older infrastructures, but they will also be subject to significant business constraints in their ability to meet customers' expectations. In an increasingly digitized economy where the management and utilization of data is central, cloud becomes an essential enabler for customer-facing businesses, including financial services. Jurisdictions that unduly constrain the use of cloud computing will place firms operating in their jurisdictions at a competitive disadvantage.

2. REGULATORY HURDLES

Those institutions that are already implementing their cloud strategies are facing considerable regulatory constraints. Such constraints can sometimes linger where a more 'traditional' view of stability prevails: where, in order to pursue the objective of promoting financial stability, some might take a static view of stability, with a bias against disruptive innovations. Amidst a landscape of increasing digitalization, it becomes necessary to view stability in a more dynamic sense, akin to riding a bicycle; ensuring stability (and with it, the maintaining solvency and protecting consumers) requires FIs to evolve and keep pace.

Furthermore, there is debate amongst some in the regulatory community as to just where cloud can actually fit under an existing regulatory structure. To some, cloud is simply a form of outsourcing, meaning that any implementation by a bank or insurer must be subject to a set of standards that were historically developed and applied to other (non-digital) outsource providers. Some other regulators see cloud more as a utility, where the CSP role is like that of an electricity supplier or a telecommunications company. But there are also other views in the direction that cloud might be considered in the future (as more material applications, processes and data are migrated to cloud) as a critical infrastructure with oversight of CSPs.[2]

These divergent views perhaps reflect the challenges of an existing framework that is geared to traditional architectures / legacy IT, and struggles to handle the type of scenarios that arise under new technologies like cloud. Concurrently, it is acknowledged that migration to cloud is not a binary decision, and the firms' strategies will consider different processes, applications or data to be migrated, such that there is a mix of cloud-based architecture and 'traditional' architecture for which the regulatory framework is more fit-for-purpose. Consequently, it may be that we need a new set of guidelines that are cloud-specific, and which can co-exist with the established regulatory framework.

[2] For instance, see keynote address by Mr Ravi Menon, Managing Director of the Monetary Authority of Singapore, at the Symposium on Asian Banking and Finance, Federal Reserve Bank of San Francisco, San Francisco, 25 June 2018 (at https://www.bis.org/review/r180727a.pdf), where he proposed the creation of a new agency specifically to regulate Cloud Service Providers. This will be further explored in our Part 3 paper.

To date, we have seen that although most regulators do not currently want to directly regulate the use of cloud (in part because given the speed of evolution of the technology and its use these would be very difficult to keep up-to-date), some requirements have started to emerge for supervised institutions migrating to public cloud (see Figure 1).[3] Those requirements generally apply in one of the following categories:

1. Scope: what can be moved into the public cloud
2. Process: how and when it can be moved to the public cloud;
3. Location: jurisdictional restrictions on public cloud location (described in Section 3).

Figure 1: Regulatory Restrictions Across Jurisdictions

The main hurdles vary across jurisdictions, whether those are restrictions that come from prudential regulation and supervision (rules for outsourcing or third-party risk management), resolution planning or from cross-sectoral personal data protection regulations. As these regulations are not specifically designed for cloud, the intensity of their impact varies by jurisdiction.

	Prohibition for core functions	Notification or Authorization	Other hurdling requirements
EU	NO	Essential functions notification	Due diligence,allow onsite inspections / clauses for operational continuity under resolution
Turkey	YES	na	na
Switzerland	NO	Notification required	Due diligence
US	NO	Notification required	Due diligence, operational continuity under resolution
Mexico	NO	Authorization required	Due diligence, allow onsite supervision / encryption of sensitive information
Chile	under revision	Authorization for material projects	Due diligence (enhance for public cloud computing), obligation to have data in country, reporting obligations
Malaysia	NO	Authorization required	Due diligence, Reporting oligations, others
Singapore	NO	Notification for material projects	Due diligence, Questionaire, Reporting oligations, others
Hong Kong	NO	Neither	Due diligence, Reporting oligations, others
Japan	NO	Neither	Due diligence, Reporting oligations, others

Scope

A central issue is the identification of material functions, meaning those functions or business services which if disrupted could threaten the viability of the financial institution, cause harm to consumers or market participants or impact financial stability.

The expanded supervisory interest in all cloud computing deployments (and not only those deemed material) has increased uncertainty about the application of regulation, raising questions about boundaries, proportionality and risk-based approaches to mitigation and compliance.

A risk-based approach is important for FIs. By basing their controls and compliance on an analysis of the risk posed by any activity or process, they can design mitigation strategies tailored to the specific risk and which allow the flexibility needed to account for the possible decrease or increase in risk posed by the activity. With

[3] Different types of Cloud deployments (public cloud and private cloud) are defined in our Part 1 paper, at: https://www.iif.com/publication/regulatory-comment-letter/iif-cloud-computing-paper-part-1

an expanded scope (such as a blanket approach that treats all cloud deployments the same), firms can lose this ability, and instead end up with maximum controls applied to all situations.

Such a situation is not only undesirable for firms owing to the significant costs involved, but it is also sub-optimal for regulators, as it does not allow firms to concentrate their resources and attention on the most important risks.

Process

In some jurisdictions, an FI needs to have a previous explicit authorization related to each case from their regulator/supervisor, while in some other jurisdictions, a notification is sufficient. A lack of clarity on legal constraints can be a discouraging factor, especially given the scale of investments in time and resources involved.

While regulators are rightly concerned about the growing use and scalability of cloud deployments, such that something immaterial could become material quickly, using this as a basis for requiring ex-ante approval does not take into account the fact that firms will already be required to control for material risks including as they develop. An FI will make the decision before scaling a deployment as to whether the change in scale results in a change of material risk and act accordingly, and regulators will already have the ability to examine this via the collection of information required in most outsourcing registers.

With these factors in mind, principles-based regulatory frameworks can benefit innovation (including the use of cloud computing) where prescriptive rules-driven approaches can not, giving firms the flexibility they need to adequately control for risks related to a fast-evolving technology in a way appropriate to their risk appetite. Where developed rules require constant review by regulators to ensure they are not out of date, key principles for financial institutions using cloud can be made to be future proof, and to address specific concerns while not constraining innovation.

3. CROSS-BORDER REGULATORY INCONSISTENCIES

Internationally, there are additional barriers that emerge from inconsistent regulatory requirements and/or additional local requirements. Several internationally-active firms have identified that while they have succeeded in meeting the requirements of their 'home' regulator for cloud, other barriers or asymmetrical treatments have prevented implementation in 'host' markets, such as the variances illustrated in Figure 1. This undermines the value proposition for cloud implementation, if the benefits of enabling enhanced analytics cannot be realized across the institution's full group.

The lack of harmonization across jurisdictions can also create regulatory and risk problems. The growing amount of information required by regulators, if unharmonized, may pose risks pushing regulators to contrasting conclusions which could have implications for the functioning of the market if, for instance, one regulator encouraged one action while another require a stop to the same action.

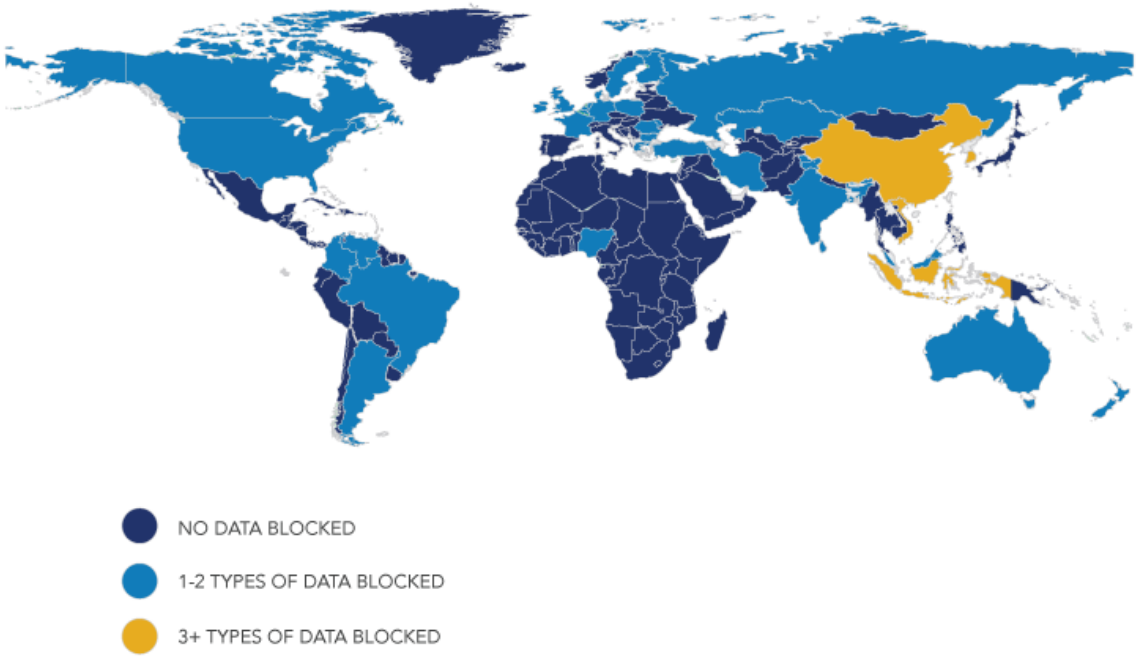
The inconsistencies that emerge are often in the migration requirements and process themselves, though they are further compounded in some jurisdictions by additional sets of home-host restrictions that apply when a specific firm wants to use cloud services in a third country.

A further (and probably the most pertinent) issue is data localization. Regulatory and legislative requirements about where data must be located and stored are important risk factors for a bank using cloud computing. A number of jurisdictions around the world are moving to restrict the residency and processing of data to within a particular country or region (see Figure 2).

In many cases, such restrictions are either local job protection measures, designed to prevent foreign agencies from accessing data without permission or measures to protect local firms from international competition. In

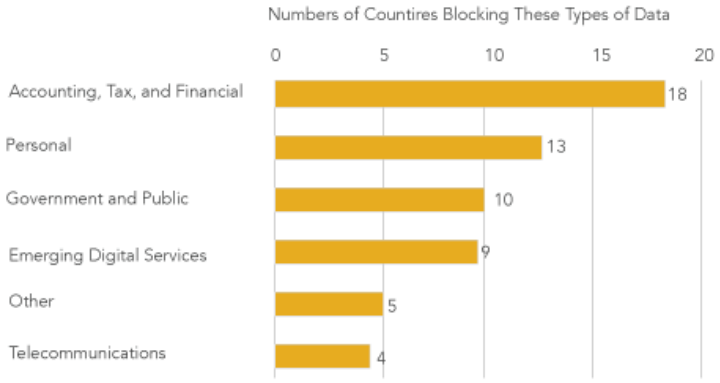
other cases, they come from legitimate concerns over a lack of alignment of privacy regulations, and a concern that national agencies may not be able to access data on citizens in a timely way. The implications are considerable, given the reach across multiple types of data (see Figure 3).

Figure 2: Countries That Block Data Flows



Source: Information Technology and Innovation Foundation (ITIF) analysis of formal laws or regulations publicly reported as of April 2017.

Figure 3: Types of Data That Are Blocked



Source: ITIF analysis of formal laws or regulations publicly reported as of April 2017.

Such policies have negative implications on the use of cloud computing, which is built on achieving scale in the storage and processing of a firm's data estate. Requirements to host data within a certain country necessitates the infrastructure required to store and process that data. Even the largest cloud providers and users do not maintain data centers in every jurisdiction in which they operate. Hence such requirements can prohibit a firm from using cloud computing for the data held in that country, which ultimately results in sub-par storage and processing of data, as well as decreased operational resilience. In the case of financial services, a firm's ability

to detect financial crime is enhanced by its ability to combine data sets from multiple countries. Continued or increased restrictions on the residency and processing of data thus risk limiting banks' ability to fight financial crime around the world.

Box 2: Non-Regulatory Hurdles

Regulatory barriers are not the only hurdles in cloud adoption, and some other potential hurdles arise within industry participants also. Common barriers include:

1. Mindset: the magnitude of the change goes beyond contracting computing power and training staff, and demands a consistent change in skills, attitude, and behaviors.
2. Skill Gaps: the skills required to operate cloud workloads efficiently and securely at scale, in areas such as modern software architectures, cloud security concepts, virtualization tools, optimization patterns for metered services and auto-scaling techniques.
3. Overwhelmed by data: mapping and architecting vast data buckets (and how to leverage it for the cloud migration process) adds complexity in a hybrid environment when on-premises legacy data systems coexist with new cloud-enabled ones.
4. Governance: cloud workflows are new and complex and require substantial planning for licensing and governance.

These cautionary notes underline how important it is for IT and business leaders to plan and invest, often needing to rebuild the business with a different architecture based on the cloud strategy they've selected.

As the strategic benefits of cloud become more obvious and compelling, and as case studies of migration experiences become more common, the organizational science of cloud implementations will continue to evolve, and some of these barriers will diminish with time, but they nevertheless shouldn't be under-estimated. Just as there is a need for regulatory progress, FIs need to be continuing their own journey in parallel.

These restrictions are all especially relevant for companies with a global footprint seeking global cloud solutions, as potential tensions may arise when dealing with a number of regulators bound to single jurisdictions and fragmented regulation.

4. CONCLUSIONS AND RECOMMENDATIONS

Cloud computing is a key element in the strategy of most FIs to face digital transformation and to be relevant in a new competitive landscape. FIs need to be able to manage and extract value from data and collaboration with 3rd parties (many of them cloud-native), with cloud adoption bringing benefits not only to incumbents but also to newcomers, to clients and to the economy as a whole.

Recommended actions for industry

On this journey, regulators have a key role in helping overcome barriers, but it is not their responsibility alone. The financial industry needs to proactively provide their own solutions to uncertainty, for instance through the creation of best practice or industry standards that could help compliance across multiple jurisdictions, such as in third party audit and the harmonization of reporting requirements.

Regulators in the UK and EU have opened the door to third-party audits of CSPs to help address concerns from both sides about managing access to sensitive data and secure locations. Where regulators have presented this opportunity, the industry needs to establish the practical terms of best practice of third-party audit, whether in partnership with the global consultancies likely to provide such audits, or in industry projects. Regulators could usefully encourage this approach by participating as observers in such projects or discussions.

Disparate reporting requirements creates significant costs for firms and can lead to sub-par regulatory decisions, though the task of achieving global harmonization is difficult, and not something that we expect the regulatory community could achieve swiftly. As such, the industry could look to create a standardized profile of regulatory requirements, similar to recent developments for cybersecurity compliance, such that compliance with any one request for information can be achieved by selecting a certain set of pre-defined fields. Ultimately the industry should be aiming for a machine-readable format that produces consistent results while significantly reducing cost for FIs and difficulties for regulators. Again, by agreeing to participate in any such projects, regulators could help encourage the development of a solution.

Recommended actions for regulators

Concurrently, there are areas where regulators can act to help address current and emerging issues. Greater clarity in supervisory interpretation of regulation is critical in enabling FIs to properly plan for how to comply, and regulators should promote a more standardized framework for cloud usage across jurisdictions.

There are some particular actions that would advance this, supported by close international coordination among banks, regulators and supervisors, firstly within the realm of existing bank and insurance regulatory structures:

1. Common set of principles: in helping regulators to develop their understandings and approaches to cloud computing from common positions, key principles should include:
    - A technology-neutral approach: the regulatory focus should be on specifying outcomes (eg. data must be protected from unauthorized access) rather than particular solutions
    - Activity based: regulatory scrutiny should focus on the specific activity that is going to be migrated to cloud, rather than on the overall concept of cloud as a whole
    - Risk-based and proportionate approaches: the scope and requirements of cloud registers should not remove the ability of firms to focus their attention and efforts where they are most warranted
    - Risk assessment and mitigation of material deployments in cloud: place the burden on FIs to determine materiality and control for it properly

    Examples of regulators with principles-based approaches can be found in various jurisdictions.[4]

2. Ongoing supervision: in some cases, the current supervisory focus is on lengthy approval process, culminating in a threshold to commence using Cloud. Both implementation efficiency and the effectiveness of risk controls would be enhanced if the primary focus shifted more to ongoing supervision once Cloud services are in operation.
3. Clarity and Harmonization: a common criterion / guideline should be developed for regulators and supervisors from different jurisdictions to validate the use of cloud to help FIs develop and imple-

[4] United States' FFIC (https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx) and OCC (https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html), United Kingdom's FCA (https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it), Germany's BaFin (https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1804_Cloud_Computing_en.html) , Australia's Prudential Regulatory Authority (https://www.apra.gov.au/sites/default/files/information-paper-outsourcing-involving-shared-computing-services.pdf), and the Monetary Authority of Singapore (http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/MAS-Issues-New-Guidelines-on-Outsourcing-Risk-Management.aspx)

ment a coherent and sound cloud strategy, especially in the case of those with a multinational footprint. This could help overcome the existing varying viewpoints on cloud (eg. as traditional 'outsourcing', as a utility, or a critical infrastructure), with a common taxonomy and harmonized notification process. Monetary Authority of Singapore (MAS) guidelines provide one example of this.[5]

4. Knowledge: expanded understanding of cloud computing and its benefits (in particular for firms' viability, and in a dynamic view of financial stability) amongst the regulatory community.

In addition, data localization requirements merit further review, seeking to expand the free flow of data to the extent possible (understanding that this requires international cooperation in data protection and security), with the appropriate security conditions and being mindful of national security considerations. This could include:

5. Transparency: on the risks that are being targeted by data localization measures: a rigorous assessment (including public consultation) of the goals, costs and benefits should precede the implementation of data localization measures, giving the industry the opportunity to address legitimate concerns through alternative means. Policy makers and regulators should consider CSPs' current data access and audit capabilities, which in many instances allow on-site inspections to regulators and make Common Service Centers (CSCs) data available when requested under a subpoena or warrant from a competent authority.
6. Free Flow of Data (FFoD): international cooperation is needed to avoid a landscape of data isolation and fragmentation. The financial regulatory community has strong experience in coordinating a global approach to policy and regulation for financial services. As data fragmentation could impact on operational resilience and ultimately financial stability, financial regulatory bodies should use their experience to create initiatives to address FFoD, such as through the Financial Stability Board.

In ensuring efficient regulation of the underlying cloud infrastructures and in enabling fair competition for all parties using those services, a cross-sectoral approach that considers:

1. Cross-sectorial and cross-border approach to CSPs: assessing CSP risks consistently and holistically, such as through other (non-financial) agencies, would ensure that specific concerns (eg. concentration risk6) will be properly monitored and managed.7
2. Potential certification of CSPs: certifying CSPS for particular activities could help to fast-track processes that are not considered critical, increasing the efficiency of the process.

[5] Monetary Authority of Singapore (MAS) guidelines on outsourcing – Jul 2016 http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

[6] According to the *EBA report on the prudential risks and opportunities arising for institutions from FinTech* (July 2018), regarding to cloud outsourcing services "ICT outsourcing risk could be also considered important, not only from the point of view of individual institutions but also at an industry or systemic level, as large suppliers of cloud services could become a single point of failure should many institutions rely on them". The report highlights also the risk of concentration in a small number of market dominant providers when using other technologies such as biometrics, robo-advice services, or big data and machine learning. In the same way, the BCBS in the report Sound practices. Implications of fintech developments for banks and bank supervisors (February 2018) mentions that "the rise of fintech leads to more IT interdependencies between market players (banks, fintech and others) and market infrastructures, which could cause an IT risk event to escalate into a systemic crisis, particularly where services are concentrated in one or a few dominant players."

[7] Part 3 of this series on Cloud will specifically address issues related to Cloud Service Providers (CSPs), including risks associated with the concentration and system-wide criticality of providers. It will also examine issues such as "vendor lock-in" CSPs' sub-contracting and Service Level Agreements, and will explore some potential regulatory responses.

Brad Carr
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

Daniel Pujazon
Policy Advisor
dpujazon@iif.com

Jaime Vazquez
Policy Advisor
jvazquez@iif.com