INSTITUTE of INTERNATIONAL FINANCE

August 2018

CLOUD COMPUTING IN THE FINANCIAL SECTOR

PART 1: AN ESSENTIAL ENABLER

1. INTRODUCTION

Customers' interactions and expectations have evolved considerably in recent years, with a greater emphasis on immediacy and personalization. This new scenario applies to virtually every interaction of customers with their environment, and financial services providers are no exception.

Financial institutions (FIs) need to adopt and actively utilize new technologies to meet such customer expectations, transforming their businesses and developing the new capabilities to become more efficient and generate more value for customers.

In this context, cloud computing is an increasingly critical element of the financial system, as the technology enabler that underpins the changes that banks and other financial institutions need to pursue. Cloud can help firms expedite processes, reduce risks and increase efficiency, as well as enhancing the ability to identify business opportunities and revenue streams, being a core element to positively impact customers through more personalized proposals, at better prices through safer and less risky operations.

This paper is the first of a series of 3 pieces that will cover key aspects of cloud technology, and the regulatory and supervisory considerations. This 'Part 1' describes cloud computing as a technology that enables companies to compete in the new financial services landscape, highlighting benefits and identifying risks and mitigants.

Significantly, it also considers the risks associated with the scenario of not migrating to cloud. Such may in fact be the highest risk scenario for a financial institution, if they are static while others are pursuing new transforming technologies and new ways of using data to open a range of new innovative and profitable business models. Concurrently, customers are increasingly building their relationship with their environment in a way where personalization and immediacy are core. Together, these two forces are reshaping the competitive landscape.

Consequently, financial institutions are defining their strategy on cloud, and the decisions are more in the "how" than in the "what". Cloud is already considered a key enabler to drive the business in the new digital playing field, and will be even more so over time. The mix on the different cloud service and deployment models will depend on each player's strategy, but the decision to at least migrate to some form of cloud appears obvious.

2. CLOUD COMPUTING TECHNOLOGY

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1] With cloud

[1] National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

computing, multiple customers share the same physical resources, securely separated at the logical level, supporting heterogeneous client platforms such as mobile devices and workstations. Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers, storage devices, and widespread adoption of service-oriented architecture and autonomic computing has driven overall growth in the cloud computing market.[2]

In general, FIs are defining their "cloud strategy", which will depend on their capabilities and size. Those strategies are created by combining the cloud deployment and service models available.

A cloud deployment model is primarily distinguished by ownership, size, and access.[3] The most common deployment models are private, public, and hybrid clouds, while the European Banking Authority (EBA) recognizes community clouds as a sub-type. While the EBA[4] definitions on the different models are very concise, they are also consistent with those provided by other public and private institutions. The **private cloud** leverages a firm's existing computer servers or, in some cases, can be hosted by a CSP (also known as Virtual Private Cloud).[5] Regardless if the private cloud is on-premise or off-premise (hosted by a CSP), the infrastructure is available for the exclusive use by a single institution. On the other end, a **public cloud** is offered by a CSP to multiple clients who share the same cloud infrastructure concurrently. Differing levels of segregation are provided depending on the cloud resources.

A **hybrid** cloud is composed of two or more distinct cloud infrastructures. The two clouds operate as unique entities but are bound together by standardized technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).[6] In a hybrid cloud, data and applications can move between private and public platforms for greater flexibility.

Finally, **community cloud** refers to an infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group.

As for the service models, the main ones are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). **IaaS** provides processing, storage and network services in a virtual environment. **PaaS** allows clients to develop and manage applications without building or maintaining any infrastructure and provides an application development and deployment environment in the cloud by offering the capability of utilizing computer programming languages and tools available from the service provider. Finally, **SaaS** provides a service that is offered directly to individuals or enterprises.

Size, technological complexity and regulation and privacy concerns set the adoption speed of cloud in different industries. Digital native companies were born in the cloud, they were in the first wave and are the most advanced in terms of adoption. They created their technology from scratch, and did not have legacy systems to be integrated - but this is not typical across industries.

The adoption progress in sectors like retail commerce or media and advertising is higher than that in the financial industry (banking and insurance). In finance, the complexity of technology is elevated, transactional core banking is highly integrated with legacy technologies, and regulation and internal governance are stricter around outsourcing and data privacy.

[2] Gartner, *Special Report Examines the Realities and Risks of Cloud Computing*, June 2008
[3] WhatisCloud.com, *Cloud deploying models*, 2018.
[4] EBA, *Recommendations on Cloud Outsourcing*, 28 March 2018
[5] AWS, *Amazon Virtual Private Cloud*, 2018.
[6] National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (see deployment models, page 7).

3. BENEFITS OF MIGRATING TO CLOUD

In identifying the potential benefits and risks of Cloud, it is important to consider the scope across public, private and hybrid clouds, and across the technology itself, the risks for individual institutions, and for the financial system as a whole. For this paper, we focus on the potential benefits and risks for FIs and for the financial sector, of the public cloud and virtual private clouds (i.e. when an external Cloud Service Provider is involved).

As with every new technology, a range of potential benefits and risks emerge. This gives rise to the challenge of assessing those potential benefits of new technologies, balanced against the identification and management of new risks - but also understanding those impacts in comparison against the existing risk profile.

Currently, financial institutions must (and are in the process to) adapt to a new reality, characterized by the customers' expectations of immediacy and personalization. The entry of new players (both in the form of start-ups, and in large established technology companies expanding their services), and the development of new business models with data at the core of any value proposition, is reshaping the competitive landscape.

In this new landscape, cloud computing is vital for competition. For established firms, a new data architecture and a technology (cloud computing) that allows for that data to be accessed rapidly are essential in order to compete with the offerings of new market entrants. In contrast, many of the start-ups entering the market are "cloud native" meaning their business and technology strategy is built around making use of cloud services offered by the major providers. For these companies, cloud computing is essential not only for what it enables, namely the speed and flexibility necessary to innovate, but also because it allows them to access computing power on demand. This enables them to therefore focus investment elsewhere, rather than in scaling the large technology infrastructure which would otherwise be necessary to compete with large businesses.

When analyzing the scenario of migrating to cloud, a number of potential benefits are identified. In the case of the providers of financial products and services (whether they are incumbent financial institutions or newcomers) the key drivers for adoption are:[7]

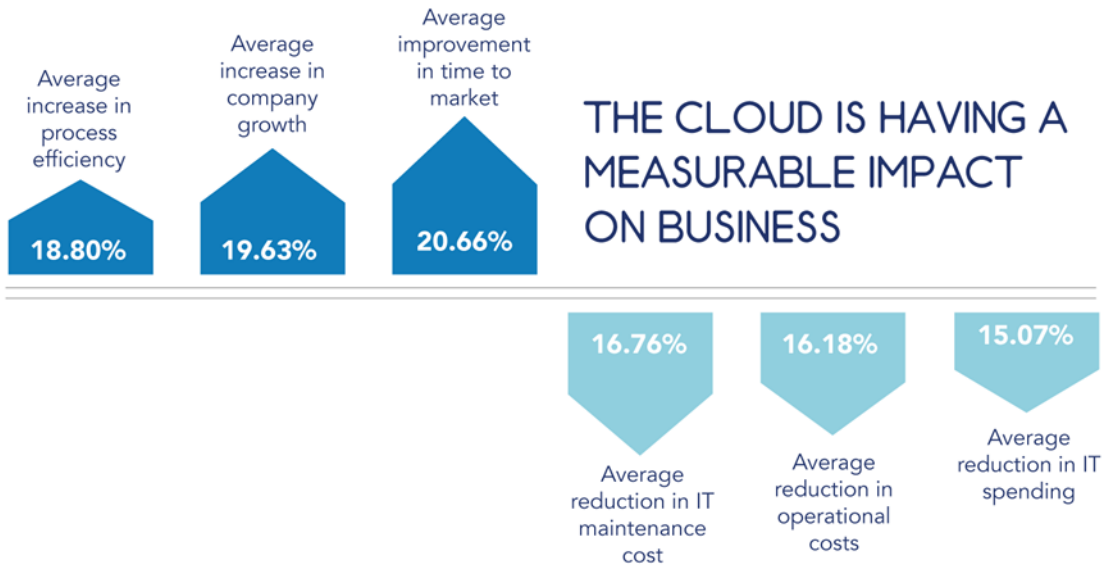
- Agile Innovation: the ability to access a shared pool of configurable computing resources can increase a financial institution's ability to innovate by enhancing agility, efficiency, and productivity. Public cloud deployments can enable financial institutions to direct internal resources, previously focused on the administration of IT infrastructure, towards innovating and delivering new products and services to market more quickly.
  In addition to that, cloud can also provide more flexibility to get into new businesses. Cloud resources provide the way to try out new ideas without extreme investments in supporting systems. A shift in business focus can be made fairly quickly.
  Finally, the time to market when introducing new proposals is also shorter, especially when you can rely on fully automated processes.
- Risk mitigation: 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 financial institutions with greater control in the management of variable IT demands, while offering new commercially viable methods to implement enhanced security controls.
- 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 financial institutions to manage computing capacity necessary to satisfy customer demand across peak periods, leveraging on a pay per use model. 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 efficiencies.

[7] British Bankers Association (BBA), *Banking on Cloud: A discussion paper by the BBA and Pinsent Masons*.

There are also a number of additional benefits from cloud that are becoming increasingly relevant in the current and future competitive landscapes:

- Since cloud solutions are global at birth, they are very well suited for multinational institutions.
- Under the new resolution frameworks that are being developed in different jurisdictions, cloud computing could provide the necessary implementation capabilities from an operational perspective.
- This new competitive landscape may also drive consolidation, and cloud is an efficient enabler for smoother mergers and acquisitions. One of the great sticking points of many mergers is the months, or even years, it takes to bring data and records from one system into another. With systems in the cloud, however, that transition is much faster.
- The FinTech ecosystems growing in many jurisdictions are characterized by "collaboration" between large and small firms. Many start-ups now entering the market are building services that are designed to be offered by scaled FIs. These companies are often "cloud native" and thus, cloud-enabled banks and insurers can manage more effective on-boarding when partnering with start-ups. A regulatory environment conducive to the use of cloud will contribute to the growth and success of FinTech ecosystems and the start-ups that populate those ecosystems.
- In a world where sustainability is becoming an extremely relevant topic, it is significant that cloud also has less environmental impact. With fewer data centers worldwide and more efficient operations, companies are collectively having less of an impact on the environment. Companies who use shared resources improve their 'green' credentials.

The benefits which come with the use of cloud computing are beginning to be realized and quantified. According to a research from Vanson Bourne, companies adopting cloud are actually experiencing quantifiable improvements in higher productivity, lower cost and improved time to market with positive impacts in the business as a whole.[8]



Source: Vanson Bourne

Ultimately these benefits will end up impacting consumers and the economy. Whether retail customers or businesses, cloud-enabled innovation in financial services can result in better products, services and an overall more seamless customer experience.

[8] Research from Vanson Bourne. "The Business Impact of the Cloud" - report compiles insights from interviews of 460 senior decision-makers within the finance functions of various enterprises.

4. CLOUD SECURITY

One key question often raised is in respect of Cloud's security. It is important to remember that the Cloud is not something "intangible" - it still requires physical servers with lots of computing power. What is different from the traditional IT infrastructure is the location of those servers, the architecture behind them and how those servers communicate with each other and with their users.

With that in mind, it is observed that many of the risks of Cloud are the same as those of any IT infrastructure, with the distinction that they are primarily under the management of a third-party provider, the CSPs.

However, it is also fair to say that the large CSPs are as secure, or even more so, than the IT infrastructures of the most advanced FIs. Security is at the core of the CSPs' business models: they have the expertise, and adequate resources both in terms of capital and personnel, evidenced in their annual expenditure to keep their systems safe, the lack of known major disruptive events, and also in their small historical downtime. Morpheus Data indicates that the total time lost from cloud outages of the 3 top CSPs in 2017 was an aggregate of just 16 hours (across all industries, not just financial services).[9]

Gartner recently identified that the improvements in cloud security will drive fewer security failures and incidents that traditional infrastructures.[10] This is already being observed, and there are many public and private firms that now rely on cloud as a more secure solution.[11]

5. RISKS AND MITIGANTS IN CONTEXT

Beyond security, it is important to consider the other main risks that FIs face when using Cloud, and how these risks are being managed and mitigated.

Operational Risks:

Operational risks result from inadequate or failed internal processes, people and systems, or from external events, and they may impact FIs in different ways. For example, data losses could happen due to failures, deletion or disasters that occur at CSPs. Of course, depending on what type of data is lost, the issue can be more or less concerning, but in most cases the vendor has redundancies in place, with the data distributed to different locations, to enable prompt recovery.

Another risk arises when developers of cloud services lack the appropriate skills, which could happen as competition to attract the best people is huge and there is shortage of expertise in the market. This skills challenge is not unique to CSPs and cloud, with banks and insurers actively engaged in such a 'war for talent' in IT and

> Cloud Service Providers and Concentration
>
> As part of this series on Cloud, our Part 3 paper will specifically address issues related to CSPs, and in particular the areas of risk that relate to a concentration of providers.
>
> That paper will include discussion on subjects such as "vendor lock-in" and the risk of a CSP operational issue having broad repercussions across multiple banks and through the system, as well as CSPs' sub-contracting ("fourth parties") and Service Level Agreements (SLAs).

[9] See Morpheus Data, https://www.morpheusdata.com/blog/2017-08-15-how-to-prepare-for-the-next-cloud-outage
[10] Gartner, *Is the Cloud secure?* March 27, 2018 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
[11] Sean Roche, associate deputy director at the CIA's Digital Innovation Directorate, June 22, 2018 https://www.nextgov.com/it-modernization/2018/06/cia-official-cloud-more-secure-old-tech-less-soul-crushing/149211/

data sciences - so the equivalent risk would arise with alternatives to cloud also. In these cases, a single vulnerability or misconfiguration could compromise all the FIs using that Cloud. This possibility is very unlikely with the biggest CSPs, but could be an issue for the smaller players.

There are also the risks associated to CSPs outsourcing some of their functions to third parties, or 'fourth parties'. FIs should be informed when this sub-contracting is taking place, to whom, and what type of information will they have access to and what services will they provide. It is important that CSPs ensure that the quality of the service, the controls in place and the security are not diminished in any way. Additionally, as the EBA cloud computing guidelines highlight, outsourcing institutions cannot outsource risk management to third parties (chain outsourcing).

All these risks can be mitigated by FIs in the due diligence process when selecting an adequate cloud service provider and when drafting the corresponding service level agreements (SLA), which will be explored further in our Part 3 paper.

One important type of operational risk to consider is cyber risk. Companies are leveraging new technologies, but so are cyber-criminals, and the use of Cloud creates new opportunities for them. As massive amounts of data are stored in cloud ecosystems, these become very attractive targets, just as banks have always been. Like banks, CSPs design their products and services with security in mind, and show a high level of cyber-resilience. Cyber risk can also be managed through risk avoidance, risk reduction, and risk transfer techniques, but it cannot be eliminated completely.[12] Financial firms must determine how to balance their business and risk decisions so that they operate within their risk profile.

As public cloud solutions become more critical and more prevalent throughout the economy, FIs and regulators need to consider how the responsibilities over the controls in place should be shared, and how to adapt the traditional enterprise wide risk frameworks to accommodate the adoption of cloud.

Financial stability risks:

In general, the risks to financial stability arising from the digital transformation of financial institutions are becoming more and more important for authorities, regulators, and institutions alike, especially when that process create single points of failure. Even though the use of Cloud by financial institutions is currently limited, it can expand very fast and become a critical infrastructure in the near future. This could be mitigated by following a multivendor strategy, so that there is no one key cloud provider for any given FI.

One additional risk is the limited number of major CSPs, and the concentration and criticality of those providers. Amazon Web Services have almost 50% market share, followed by Microsoft Azzure, Google, IBM or Alibaba, and this concentration may be further exacerbated by constraints on the ability to switch from one CSP to another. This will be further explored in our 'Part 3' paper.

Other risks:

Among other risks, it is important to ensure data portability and interoperability within the cloud, amidst the large number of competing cloud technologies for data storage and retrieval. Each technology carries the risk of what is commonly known as the "vendor lock-in", where an FI is dependent on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities. That means that FIs have more difficulties to move data into,

[12] IMF, *Working Paper: Cyber Risk, Market Failures, and Financial Stability*, August 2017.

around and out of the cloud, as well difficulties if for any reason they want to exit their cloud (i.e. if a CSP decides for business reasons to stop providing cloud services, etc).

There are currently tools and techniques that help mitigate those risks and keep data in the cloud accessible and portable, which we will explore in more depth in our Part 3 paper.

6. RISKS OF NOT MOVING TO CLOUD

Risk analysis would not be complete without examining the consequences for an institution that does not move to Cloud.[13] As well as security risks, there is the business risk: the risk of being left behind.

Security and Continuity Risks

Any IT infrastructure has vulnerabilities, and keeping the traditional mainframe architecture does not guarantee a higher level of security compared to cloud. On the contrary, some of the traditional IT risks become much more relevant if financial institutions want to keep up with their customer expectations.

Among those risks, perhaps the most important is not having enough computer capacity to store and process the huge amount of information now required to provide a personalized experience. Redundancy is key as well, as cyber-threats are on the rise and institutions need to plan for back-up mechanisms that allow them to get back to business as soon as possible. That requires both capacity and resources, especially if that is done in-house. Institutions must have a high level of operational resiliency, and that is more difficult to achieve running obsolete systems in the new very demanding environment.

Not pursuing the migrating to Cloud would involve retaining legacy systems that are static, expensive to maintain and update, and not designed to cope with the structural increase of demand or with unexpected peaks of demand and that require months to provision for infrastructure.

Business Risks

The main risk comes from not giving enough importance to the drivers behind the transformation of the financial industry, from the market and customer.

Within the competitive marketplace, there is the increased regulatory pressure on financial institutions and the observable impact in their profitability. Simultaneously, new big players are entering the most profitable parts of the value chain using the most advanced approaches, leveraging new transforming technologies, as well as the new ways of using data that open a range of new innovative and profitable business models.

On the customer side, the landscape is also changing rapidly. Customers are increasingly used to digital experiences in other sectors, so they expect to be able to do banking anytime, anywhere; to get proactive and personalized help with their finances; and to interact with their banks seamlessly through multiple devices and applications, seeking always the best possible experience.

The combination of all those factors underpins the need for banks to adapt to the new trends, or risk being left behind, both by peers and new entrants. Banks need to be able to test innovative products and services, make

[13] These risks of not moving to Cloud are considered in a broad sense, inclusive of the public, private and hybrid cloud scenarios.

them available to the market globally, with speed to market, and at a reduced cost, while keeping high standards in quality and reliability. To do so, they must leverage the new technologies available, among which large-scale use of big data, artificial intelligence and cloud computing are key.

The strategic imperative of moving to cloud is only partly about reducing cost and increasing efficiency, and more importantly about meeting customers' expectations, and being able to compete in the increasingly open and dynamic marketplace. This is ultimately the most critical driver to maintaining a viable (and hopefully thriving and profitable) business.

7. CONCLUSION

The criticality of data and data management in the digital economy is especially evident in the financial services industry. This is a central determinant not only for which firms will thrive as market leader, but also in their ability to keep pace and survive.

Cloud computing is a key enabler in the management of massive datasets, and it presents numerous benefits and opportunities in meeting evolving customer expectations. Like any new technology, it invariably has risks – but the biggest risk may in fact be the risk of not moving. The financial institutions that don't pursue migration to cloud computing will need to support older infrastructures, and suffer significant business constraints in their ability to service customers. The cloud strategy questions are not about "if," but rather "how."

The key considerations then, both for FIs and for their regulators, are (i) the practical hurdles (both regulatory and non-regulatory) in migrating to cloud, and (ii) Specific issues associated with cloud service providers, including concentration and dependency. These two areas will be the specific foci respectively in the IIF's upcoming Parts 2 and 3 papers.

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