SESSION SUMMARY - BUCHAREST APRIL 2019

Cloud outsourcing: opportunities and challenges

1. The benefits and opportunities provided by cloud technology in the financial industry

1.1. The main benefits of cloud computing

A regulator stressed the increasing rate of adoption of cloud outsourcing in the financial industry. An EBA assessment in December 2018 conducted mainly among the larger banks in the EU found that cloud computing is an important driver of business for these banks. Over 50% of respondents have adopted cloud computing for some part of their activities. Another 30% were considering it or planning for it, and only a small proportion had no plans to do so. An industry representative noted that people often say that financial services companies are increasingly becoming technology companies, but the reality is that they want to be able to leverage and harness technology, but they do not fundamentally want to become technology companies.

Several speakers detailed the benefits provided by the use of cloud computing services in the financial sector.

Cost is a first factor. An industry representative stated that cost reductions are a major motivation for businesses using the cloud, but many of them have not yet managed to realise all the benefits in this respect. This is largely because institutions have sought to replicate the same types of technologies and the same ways of implementing them in the public cloud that they have used historically rather than conceiving new ways to leverage technology. Another industry representative felt that there could be cost benefits in the form of future cost avoidance. If a business information system is moved to the cloud, it will require less additional investment in 5 or 10 years.

Improving scalability and time to market is a second potential benefit of cloud computing. An industry representative explained how the modernisation of IT systems using cloud-services can support shorter time to market, create faster business services to customers and create a more internally agile organisation while also providing a scalability benefit. In terms of time to market, with cloud-services businesses can create services or applications on a small scale in one country and then expand them easily across the world or on the contrary decrease the service if it proves inefficient or if activity drops in the future.

Thirdly, the cloud also facilitates innovation. An industry representative considered that the venue for exploiting new technologies such as Distributed Ledger Technology (DLT), Artificial Intelligence (AI), machine learning, enhanced and next-generation data and analytics, automation and robotics will increasingly be the public cloud because it is impossible to leverage some of those capabilities within a traditional technology environment. One of the prerequisites for institutions being able to leverage these new services is the availability of large amounts of data which only exist in the public cloud. Quantum computing is another area where great progress is expected over the next five years and which institutions are expected to leverage mainly as a public-cloud-service. Another industry representative added that the cloud allows businesses to utilise these technological innovations with far less investment than if they were to do this alone. The cloud also allows a business to change the way it functions internally and externally more easily and rapidly.

1.2. Future development of cloud computing in the financial sector

An industry representative stressed that simply moving existing applications and systems to the cloud does not allow institutions to reap all the potential benefits offered by the cloud. This does not achieve cost reduction, is not innovative and certainly does not transform an institution's business model. Rather than replicating what was done in the past, businesses are now seeking to exploit new platforms and capabilities. Firms would be able to enjoy more fully the benefits of the cloud if they move away from infrastructure as a service, which is akin to how IT is delivered to enterprises today, towards software as a service (i.e. providing access to application software from any device with an internet connection and web browser – see Appendix for definitions). This is the case notably with new technologies such as AI, machine learning and smart analytics. An increasing number of fintechs are expected to offer software as a service propositions in the future, as some services become less differentiating and institutions will need to use the public cloud to access these technologies. A regulator also saw many benefits with the use of the cloud in terms of innovation and increase in data-analysis capacity. For the first time, some firms are seeing the value of their data and understand how it can benefit their business. They are also using the cloud to transform their business. The cloud is a substantial shift in how IT technology employees operate. Rather than having a linear production line of monthly releases, they are moving to more agile dev op teams which are able to respond much more quickly with more frequent releases.

1.3. From a basic utility to a more sophisticated service

A policy-maker drew an analogy between cloud-services and the provision of electricity. If the panel were taking place in 1919 rather than 2019, there could have been a similar discussion about the adoption of electricity by the banking system. An industry representative broadly agreed with this analogy. Increasingly, the technology now available in the cloud is essentially a utility service provided in a cheaper and more innovative way. Key regulations are driving this behaviour. For example, FRTB (the Fundamental Review of the Trading Book), which particularly affects capital-market institutions, requires an eightfold increase of IT infrastructure spending by some institutions to comply with the regulation, due to the enhanced risk modelling and the number and frequency of calculations required, as well as the amount of data involved. In a banking environment with depressed returns on equity and capital and diminished IT budgets, it does not make sense to make this kind of investment in technology.

An official however considered that the analogy with an electricity utility does not hold true for several reasons. First, electricity is produced locally rather than on other continents. It is a regulated industry and institutions know what they are purchasing. From a supervisory perspective, the supply of electricity has a simple solution in terms of business continuity with the installation of an emergency generator. That is quite different to the cloud, and it poses a number of questions about the regulatory framework needed for the cloud. In addition, institutions using

the cloud for relatively sophisticated applications such as analytics or the provision of essential software, must be aware of how the analytics are produced, unlike with electricity. The policy-maker agreed that the utility analogy mainly holds for fairly basic applications of the cloud.

2. Existing regulatory and supervisory framework at the global and EU levels

2.1. Existing frameworks at the international level

An official commented on the results of a study conducted by the Financial Stability Institute (FSI) of the BIS on the regulatory and supervisory approaches to cloud computing in the insurance sector in Europe, Asia and North America[1]. Three main approaches were identified relating to outsourcing; governance and risk management; and information security. Cloud computing is generally considered in existing frameworks as a form of IT outsourcing if the outsourced function or activity is material. However, the materiality criteria are different between jurisdictions and are frequently unclear regarding cloud computing. In jurisdictions where cloud computing adoption by financial institutions is increasing, some authorities have enhanced their approach by clarifying their regulatory expectations regarding the use of cloud computing and addressing the specific risks posed. There is value in this approach. Some authorities have allocated specific cloud sections in the regulations with binding requirements while others have published specific guidance, recommendations, information papers and discussion papers.

These cloud-specific provisions or recommendations do not regulate the technology itself but the underlying governance and risk-management framework and mainly focus on six areas. The first area is the materiality assessment of the arrangement. Besides taking into account the outsourced function or activity, authorities recommend considering the type of deployment model[2]. The second area of focus for authorities is the due diligence of cloud-service providers and what it takes into account[3]. The third area relates to the risk assessment of the cloud solution, in which authorities expect institutions to classify risks and determine the actions they will take to mitigate these risks. The fourth area relates to data location, in the sense that authorities generally recommend that institutions understand the legal environment of the jurisdictions in which their data will be located and processed. In some cases, authorities even require that institutions' particularly sensitive data should be hosted locally. The fifth area is about business continuity and exit plans. Authorities require institutions to include in their contracts performance and service levels, such as maximum downtime or processes for the removal and deletion of data at the end of a contract. Finally, the sixth area is urgent access rights, where most authorities require a specific clause that grants access to the insurer concerned, its auditors, data and business premises.

In the EU, the FSI observed that most national supervisors in the insurance sector consider the EBA recommendations on outsourcing to the cloud as a reference and EIOPA has decided to develop guidance based on these recommendations, with minor adjustments related to the specific risks of insurance. The FSI concluded that there are three main considerations for all financial authorities to take into account. First, there is value in clarifying regulatory expectations in order to address the potential specific risks associated with cloud computing and to support market participants in the responsible adoption of the technology. Second, supervisory frameworks must be enhanced to ensure that authorities assess and monitor the specific concentration risks arising from the market structure of cloud providers. Third, international cooperation is essential for the effective oversight of cloud-computing activities in the financial sector.

2.2. The EU's regulatory approach

A policy-maker stated that the Commission supports the transition to a cloud-based economy, but this transition must happen within a regulated framework. The EU legislation that underpins this subject is the free flow of non-personal data regulation, known as the fifth EU freedom, which was adopted last November and comes into force in May 2019. Some sector-specific requirements may be needed. In the financial sector there are three main areas of focus: security, data protection and the reliability of cloud-services. This is why the Commission welcomed the EBA recommendation on outsourcing to cloud-service providers, published in December 2017, which has been integrated into revised guidelines on outsourcing in February 2019. A regulator added that the EBA's assessments have indicated that there is a correlation between clear regulatory frameworks and the appropriate use of cloud. This concerns primarily the larger institutions but can also be of relevance for the smaller ones.

3. Challenges posed by the increasing development of cloud-services and potential need for additional guidelines

3.1. Potential risks posed by the development of cloud services

A regulator outlined the main risks posed by cloud computing. These concern data security, data protection and the disruption of systems. Requirements for providing cloud-services for the regulated EU financial-services sector need to be clear, even if there is not a total alignment among regulators and industry players on all points across the Union, because this clarity facilitates the use of the cloud within the EU financial sector. There are also other risks around control over access, residency and concentration risk, another regulator added, which are being monitored by supervisors in the EU. An official considered that the established industry players are not the most concerned about the reliability and security of cloud-services. Feedback received from the market suggests that disrupters and new companies such as fintechs seem to be the most interested in an additional regulatory framework defining the type of service it is safe to use. In terms of other areas such as data protection and encryption standards, there are issues about the reliability of services. Interactions in cases where institutions use the cloud as an essential software service or for analytics are also relatively complex.

An industry representative noted that there are still many concerns about moving large amounts of data into the public cloud in regulated industries such as financial services, which is necessary for reaping all the benefits offered by the technology. This raises questions regarding what access cloud providers have to customer data, what they may do with it, where it is located and whether it is communicated to anyone else, illustrating the difference between cloud computing services and typical outsourcing. The speaker's company – a major cloud provider – endeavours to be as transparent as possible on these different elements. The industry speaker also highlighted the importance of security, noting that the public cloud has incorrectly been perceived as less robust than a traditional infrastructure environment. Security in the

[1] FSI Insights on policy implementation N°13 - Regulating and supervising the clouds: emerging prudential approaches for insurance companies - Financial Stability Institute - December 2018.

[2] i.e. whether it is a public, community or hybrid cloud; whether it is an infrastructure, platform or support service, which involves different shared responsibilities and also the level of criticality or sensitivity of the data stored and processed in the cloud.

[3] i.e. the adequacy of the cloud-service provider's risk management and internal control procedures, compliance with data protection and data security regulations, and the adequacy of their recovery plans.

public cloud is at least comparable if not higher than in traditional environments given the significant investments public cloud providers make e.g. in terms of employing large teams of security engineers and putting in place elevated security models.

3.2. The division of responsibility between cloud providers and their customers and the role of supervisors

A regulator considered that outsourcing to the cloud entails a shared responsibility which can be stronger than in other types of relationships. There are many different types of services in the cloud (e.g. infrastructure as a service, software as a service, platform as a service). Firms need to define who is responsible for what and where the shared responsibility lies to ensure that governance and accountability are clear and to avoid gaps in security and incident management. In terms of responsibilities, the speaker felt that outsourcing to the cloud should be considered as any other third-party outsourcing arrangement. A firm should remain responsible for its own operational resilience and business continuity and also its outsourcing arrangements and therefore cannot contract out its regulatory obligations. This was set out in the FCA's 2016 cloud guidance. In addition, as part of its oversight on operational resilience, the FCA, jointly with the Bank of England, has issued a discussion paper on operational resilience, which is also relevant to technology-related outsourcing. Firms should be able to absorb shocks rather than contributing to them and therefore they should understand how to restore business services in case of disruption and make the investments required in order to ensure resilience.

Another regulator stressed that the EBA's outsourcing guidelines are relevant for all types of outsourcing and notably cloud outsourcing. Different layers of activity can be outsourced to the cloud, from infrastructure only to the full package. Even if a firm is only making use of the cloud for infrastructure, it will still have to apply the rules, but this can be done in a proportionate way. This might make exit planning easier to manage, but security and availability will still remain an issue. The intensity of the rules can differ depending on the type of outsourcing, but the EBA's basic principle is essential: firms remain responsible for the activities they outsource. An industry representative felt that the model of shared responsibility in the public cloud poses a question over where the boundary lies between the responsibilities of cloud-service providers and customers in a context where increasing amounts of responsibility could potentially be delegated to cloud-service providers. This requires transparency on the part of cloud providers in terms of how the data is handled and what type of access cloud-service providers have to it. Another industry speaker added that companies using cloud-services must also prepare appropriately their internal processes and organisation in order to achieve the best outcomes from cloud use.

3.3. The possible need for additional or more specific guidance on the provision of cloud-services

An official explained that fintechs would prefer a licensing system establishing standards to be met by cloud-service providers that are safe to use. This would allow them to use these services without having to bother about assessing them. Supervisors however are usually not favourable to this approach, because it allows the management to exonerate itself in the case of a problem, by blaming the cloud-service provider. On the other hand, it is difficult for the full responsibility to lie with the management of institutions outsourcing to the cloud, particularly in the case of fintechs which are small companies that have very unfavourable negotiating power compared to the major foreign cloud providers. It might be beneficial to have a European framework to express the essential requirements for cloud-service providers. This framework would describe the minimum standards for the provision of these services, but not a 'sufficient' standard because some responsibility must remain with the company outsourcing. It should include, for example, the requirement for companies to allow access to supervisors. Another issue is when the usage of data is outsourced completely and the institution does not understand the algorithms being used, it will be impossible to hold managers accountable for business decisions taken on the basis of this analysis. In that scenario, it is important to think about the distribution of responsibilities and to determine what standards should govern the interactions between cloud users and cloud-service providers.

An industry representative suggested that a certification process could be used in order to support the adoption by European countries of some cloud providers and emphasized that several important topics need considering in regulation. First, there is no single regulation on cloud in Europe; harmonisation in this area would be highly beneficial across sectors and jurisdictions. The cloud introduces a new paradigm, especially in respect of access to data, allowing institutions to classify information and put it in the right place. There is also a question concerning data retrieval and the related time and flexibility, because data needs to be provided at the most appropriate time. The US CLOUD Act is another issue and how it will interact with European regulation such as GDPR.

A regulator suggested that any set of rules or framework should be harmonised, but principles-based and high-level, and perhaps supported by guidance, in order to keep pace with innovation and developments. Otherwise, it will very soon become out of date.

Another industry representative mentioned some issues that might require further guidance. First, there are specific transparency implications in relation to shared-responsibility models in the context of 'software as a service' provision that need considering. The users of that type of service do not need to really understand how the service functions, however, financial services firms will need to be able to prove to regulators how they are operated. Obtaining prescriptive guidance from regulators about the evidence that is needed would be very helpful. For example machine learning and AI are increasingly being used in "software as a service' solutions. Efforts are being made to increase transparency and eliminate biases and it would be useful to know how to evidence this. Secondly, there has recently been helpful guidance on encryption and the requirements for data moving into the cloud. If data is moved in support of materially outsourced workloads or applications, should it be encrypted? If it is encrypted, how should the encryption be enacted? Does the customer of the encryption key retain control or should this responsibility be devolved to the cloud provider? Prescriptive guidance from regulators on this topic would be very useful also.

3.4. Potential data location issues

A regulator suggested that the EBA has taken a very risk-based approach to data protection in its guidelines, which is sufficient and suitable for both the sector and the cloud-service providers. Having more specific location requirements is undesirable, as there are other ways to protect data. An industry representative felt that the issues around data localisation remain a barrier to the uptake of cloud-services in Europe. A solution adopted by some large cloud providers is to have datacentres in different European countries, but there will always be business locations where there is no data-centre presence. One of the key solutions here might be open-source technology, for example.

3.5. Financial stability issues

A regulator noted the EBA's responsibility for the macroprudential side of the cloud. There are macroprudential concerns in terms of cyber-risk, but the 'elephant in the room' in terms of financial stability is potential concentration risk. A question is whether a specific regime is needed for these providers. The ESAs will shortly be providing joint advice to the European Commission regarding potential legislative improvements in this area. This

proposal considers the establishment of an appropriate oversight framework for monitoring critical service providers. This process is still in the very early stages of development, however. This is a complicated issue, but some of the thinking in this proposal will soon be delivered and made public. It is also important to consider what is happening on a global level.

Concerning the potential concentration risk, an industry representative explained that enterprises increasingly leverage multiple cloud providers, which begins to address this risk. The speaker's company provides guidance to financial services institutions on how to take advantage of multiple cloud providers, recognising the requirement from regulators not only to mitigate concentration risk but also to address issues such as exit strategy. In the event of a commercial failure, for example, an institution might need to move its materially outsourced workloads or applications to another cloud provider. Cloud-service providers need to engage with regulators and prospective financial services customers on how this can be done.

Appendix:
overview of cloud computing[4]

In common terms, cloud computing could be defined as a model that enables on-demand network access to a shared pool of configurable computing resources. The US National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications or services) that can be rapidly provisioned and released.

According to NIST, cloud computing has five essential characteristics, three service models and four deployment models.

Five essential characteristics

The main characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service:

- On-demand self-service: users are able to access computing resources without any human interaction with the service provider.
- Broad network access: computing resources are accessible over the network, supporting heterogeneous client platforms (e.g. mobile devices and workstations).
- Resource-pooling: the provider's computing resources are pooled to serve multiple users under a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand.
- Rapid elasticity (scalability): capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward, commensurately with demand.
- Measured service: cloud systems optimise resource use by leveraging and metering their capabilities appropriately according to the type of service. Resource usage can be monitored, measured, controlled and reported, providing transparency for the provider and user (pay-by-use).

Three service models

There are three main types of cloud-service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS):

- Infrastructure as a Service (IaaS). Providers offer access to computer infrastructure resources as processing power, storage, servers, networks and other resources where users are able to run an operating system with applications of their choice on it. Virtualisation allows many users to share one physical server. Users have control over storage levels, operating system and specific network components.
- Platform as a Service (PaaS). Providers offer a computing platform where users can run and develop their own applications using libraries, languages, databases, tools and other providers' resources. This option provides users with tools for developing new online applications. Users have control only of their own applications that run on the platform plus the platform's configuration settings.
- Software as a Service (SaaS). Providers offer access to application software from any device with an internet connection and web browser. Off-the-shelf applications are free or paid via a subscription, accessed over the internet from any device, facilitating collaborative working. Users have control only of configuration settings specific to the application.

Cloud computing services are constantly evolving. As emerging technologies evolve and are applied to different use cases, new services are being offered, such as Business Process as a Service (BPaaS), Cloud Management as a Service (CMaaS), Blockchain as a Service (BaaS) or the recently launched Quantum Cloud-services.

Four deployment models

Cloud computing can be deployed in different models according to the type of use. There are four types of deployment model: private, public, community and hybrid. The main differences between these deployment models relate to the availability of the cloud infrastructure:

- Public cloud: available for open use by the general public.
- Community cloud: available for the exclusive use by a specific community of users from organisations that have shared interests.
- Private cloud: available for the exclusive use of a single organisation.
- Hybrid cloud: composition of two or more distinct deployment models that retain unique infrastructures but are interconnected. ●

[4] Source FSI Insights on policy implementation N°13 – December 2018