Cloud and tech outsourcing

Denise Garcia Ocampo

Senior Advisor - Financial Stability Institute,
Bank for International Settlements (BIS)

Enabling the potential of cloud computing through effective oversight frameworks

In an economy where consumers expect speed, tailored offers, attractive pricing and user-friendliness from products in every industry, the financial sector is no exception. Financial institutions are increasingly relying in digital technologies to be able to respond timely and efficiently to customer expectations. To achieve this, financial institutions require significant computer resources to be able to analyse large volumes of data, identify patterns and trends in that data and process the necessary algorithms.

In this context, cloud computing is an IT model that enables financial institutions to use digital technologies under an efficient, scalable and flexible scheme. Through a cloud computing model, institutions have access to available-on-demand shared networks, servers, storage, applications and services that can be rapidly scaled up or down and accessed anytime and anywhere. Benefits will depend on the use and type of model being deployed, but in general cloud computing may bring savings in IT costs, access to qualified talent and tools, flexibility and facilitation of innovation.

> *"Contagion in the event of a large-scale operational failure and possibly posing systemic effects."*
>
> \- DENISE GARCIA OCAMPO

However, the use of cloud computing may increase a number of risks for financial institutions. To begin with, operational and reputational risks. These risks are connected with failures in data security and privacy, system availability, continuity of operations, auditability and compliance with legal requirements. Moreover, business continuity of financial institutions and resiliency of third-party service providers are major concerns when relying on cloud computing, given that cyber-attacks and outages may impact the provision of financial services.

There are also key concerns related to concentration risks. A growing number of financial institutions as well as other IT third party providers are relying on a relatively

>>>

>>> small and highly dominant pool of cloud service providers, increasing the threat of contagion in the event of a large-scale operational failure and possibly posing systemic effects in the financial sector. Access and audit to third party providers and data is another key concern, since location in different jurisdictions may complicate the effective oversight of cloud computing activities.

Against a background of potential benefits and risks, a recent FSI Insights paper "Regulating and supervising the clouds: emerging approaches for insurance companies" analysed the prudential approaches taken by selected financial sector authorities to deal with cloud computing. The analysis showed that authorities usually apply their frameworks for general outsourcing, governance, risk management and information security to cloud computing. Some authorities include cloud-specific sections in these frameworks, while a meaningful number have issued cloud-specific recommendations or supervisory expectations. Regardless of the approach taken, cloud computing arrangements are subject to regulatory requirements only if they are deemed as material. However, the criteria for deciding whether such arrangements are material vary across jurisdictions.

Regarding the supervision of cloud computing, these arrangements are generally part of the oversight of operational risks and authorities follow a risk-based approach. Before an institution enters into a cloud servicing agreement, some authorities require notification, while others prescribe a consultation or approval process. At the very least, most authorities expect informal communication from financial institutions on their material cloud computing plans. Authorities are also using thematic reviews and informal contacts with cloud providers to complement their oversight of the cloud computing business.

With respect to future cloud computing challenges for authorities, the FSI paper highlights the following:

(i) reviewing regulations to strengthen the institution's governance and risk management requirements;
(ii) developing supervisory tools to assess concentration risks of cloud providers in individual and aggregate levels, as well as a cross sectorial analysis;
(iii) implementing tools to assess operational resilience for both institutions and their IT third party providers; and
(iv) enhancing cross-border cooperation, particularly in terms of information-sharing, as an essential element for the effective oversight of cloud computing risks and the implementation of orderly resolutions. ●

Levin Holle

Director General, Federal Ministry of Finance, Germany

Cloud computing: challenges to regulation by new IT infrastructures?

Internationally competitive economies cannot evolve without the division of labour. This goes hand in hand with the breaking up of value chains and is especially pertinent to information technology. The necessity of a division of labour is particularly striking when it comes to cloud computing.

In times of intensifying digital financial innovation, cloud computing services offer several advantages: the basic layers of information technology, i.e. running the underlying machines, storage, operating systems and even applications, have become increasingly standardised, leveraging economies of scale and significantly lowering the cost of operation as a consequence. This effect allows financial institutions to devote more attention to the development of custom-made financial applications that >>>

>>> are tailored to fit specific business models. Additionally, cloud computing makes it significantly easier for small new companies, e. g. FinTech companies, to enter the financial services market: They can source the IT services they need at prices they would not be able to achieve themselves if they had to set up the complete infrastructure on their own. Cloud computing is thus enabling competition and new business models.

However, cloud computing – like all forms of outsourcing – inherently reduces the level of control exerted by the respective financial institution, even if they retain the responsibility. Furthermore, the use of a limited number of global cloud providers by multiple financial institutions could lead to concentration risks, which could, in the long run, have implications for financial stability. This creates new regulatory challenges for financial institutions as well as for competent authorities. Since reliance on cloud computing is rapidly increasing, a closer look at dependencies between the financial sector and third-party IT service providers is important.

In a bid to address these risks, the European Banking Authority (EBA) recently issued a recommendation on outsourcing to cloud service providers. Additionally, the German Federal Financial Supervisory Authority (BaFin) has published guidelines for compliant cloud service provider outsourcing. The German FinTech Council's recommendations propose a European tech licence for cloud computing service providers offering services to financial institutions.

If we want an innovative European single digital market, it is essential we embrace the advantages of cloud computing while also mitigating the risks. A harmonised approach to cloud computing tackling these issues would contribute to the EU´s competitiveness. ●

Nausicaa Delfas

Executive Director, International, Financial Conduct Authority (FCA)

Cloud and technology outsourcing: issues for regulators

Regulators across the world have long focused on the importance of robust controls and oversight by regulated firms and markets of their outsourcing arrangements. Such outsourcing has historically covered a range of business support services and activities: from human resources to IT infrastructure, payments to platforms, through to back-office functions. But as technology has developed, so have opportunities to outsource functions, the way in which outsourcing is delivered, and the range of third parties who offer services.

So, to an extent, outsourcing to the Cloud and to other third-party technology service providers is just another form of outsourcing. But Cloud and technology-related outsourcing do pose their own challenges for firms and regulators: including where these involve business-critical services, or where they could pose concentration risks. Despite the common basic features of the Cloud, there are also a range of different deployments (e.g. public, private or hybrid) and service models.

Using Cloud services can bring benefits such as: cost reduction; increased deployment speed; global scale; better performance and improved resilience. But it can raise new risks, such as the potential for lines of responsibility to get blurred between >>>

>>> the firm and its vendors; loss of control regarding data encryption, access, destruction and residency; and vendor concentration risks.

One of the largest sources of disruptive incidents reported to us relates to services provided by third party service providers. Contractual arrangements with third parties are often complex and longer term because of the services provided (and supply chains often extend across borders); and third-party providers can sit outside the regulatory perimeter for some of their activities (or may be covered by other regulators in the case of e.g. utility or communications services).

The FCA was one of the first regulators to issue guidelines to clarify how our existing outsourcing standards apply to the Cloud (FG16/5) and similar services. Existing requirements and guidance are broadly that:

- regulated entities must take responsibility for their third-party service providers;
- firms cannot contract out of their regulatory obligations and are expected to manage risk;
- firms must take reasonable care to supervise the discharge of outsourced functions by a third party, and should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls.

Such high-level principles remain valid. The FCA has recently published, with the Bank of England, further consultations focused on operational resilience issues (DP18/04). We expect firms to plan for "when" rather than "if" a disruptive event occurs – with focus on firms' "impact tolerance", and their recovery and response, as well as defence.

We continue to closely monitor the risks from the provision of cloud services to the financial sector – and we continue to contribute to international work on outsourcing, such as the current review of IOSCO principles on outsourcing by markets and market intermediaries, and recent EBA guidelines on outsourcing in banking. ●

EUROFI PRESIDENT // David Wright
SECRETARY GENERAL & PUBLISHER // Didier Cahen
ASSOCIATE PUBLISHERS // Jean-Marie Andrès and Marc Truchet

EDITORIAL COORDINATORS // Virginie Denis and Cristian Matei
GRAPHIC STUDIO // Initial Production - www.initialproduction.be