Cloud based platforms

Lie Junius

Director of Government Affairs and Public Policy, EMEA, Google Cloud

Solving for better financial services for the European consumers: technology trends and policy considerations

The use of cloud-based technologies is a key pillar of the digital transformation of the economy, driving competitiveness and generating significant economic and social benefits[1].

Trends and benefits

Ultimately, it is the European consumers that stand to benefit the most from cloud-enabled financial services. Innovative financial services providers can create experiences that more closely resemble the best digital ones in other industries.

Today's digitally savvy banks are using the cloud to process vast quantities of information to rapidly construct and sell financial products that differentiate themselves in a highly competitive market. Cloud is reshaping the technology landscape, and it has the potential to transform financial services beyond core infrastructure.

One of the main challenges that the financial industry (and their regulators) is working to address, with the help of cloud, is management of the extremely large volumes of data across the organizational silos and accelerating time to insights.

Also the financial sector can utilise the cloud to become more capable at combating fraud and money laundering. By using more dynamic artificial intelligence (AI) and machine learning (ML) models, rather than static rules-based systems—combined with transactional and behavioral data—banks can now more accurately detect evolving fraud patterns while avoiding costly false positives.

As a recent development, COVID-19 is rapidly changing how financial services institutions serve their customers, empower their workforce with remote work capabilities, and adapt to new market and economic risks.

Challenges to adoption

It is important to take into consideration that most financial institutions across Europe and globally, are at an initial stage of their cloud journey. And the vast majority of initial application of the technology is happening in the area of non-material outsourcing, as confirmed in a recent report by the Financial Stability Board[2].

Whilst financial sector institutions have traditionally been early adopters of the private cloud, they have been relatively slow to migrate to the public cloud due a variety of factors including the complexity of the regulatory landscape and difficulties associated with migrating from legacy infrastructure. These issues are compounded by the concerns over the risk of the vendor lock in, and a variety of perception challenges including around data residency and access. Understanding and navigating change management and upskilling workforces, as well as raising the cloud-specific expertise and trust levels within senior decision makers and board-level stakeholders, are two other critically important factors that cannot be underestimated.

Nevertheless, adoption of public cloud services has gradually increased over the past few years, as financial institutions have realized the business and security benefits of making the shift, and many initial concerns were eased by the cloud service providers' stronger compliance programmes. Banks like Lloyds, Deutsche Börse Group, HSBC are accelerating their cloud innovation, in partnership with Google Cloud.

> *Cloud adoption in finance is accelerating, but further efforts are needed to raise trust and understanding of security and operational resilience of the cloud.*

Security and operational resilience of public cloud

The adoption of public cloud technology can augment security. Recent research from McKinsey[3] concludes that organisations expect to double their public cloud adoption due to the growing understanding that cloud platforms' security capabilities have surpassed those available on premises.

Similarly, cloud providers that develop and offer to their customers highly redundant and resilient systems by design, are well prepared to cater for the business continuity and disaster recovery needs of the financial institutions.

Application of multi-cloud strategies also supports financial institutions in addressing vendor lock-in concerns and enhancing operational resiliency capabilities. ●

1. Deloitte: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf
2. https://www.fsb.org/wp-content/uploads/P091219-2.pdf
3. McKinsey. Making a Secure Transition to the Public Cloud: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Making%20a%20secure%20transition/Making-a-secure-transition-to-the-public-cloud-full-report.ashx

Kaj-Martin Georgsen

Head of Corporate Responsibility & Public Affairs, DNB Bank ASA

A future-proof, customer-centric banking system needs to tap into the cloud

Reaping the benefits of cloud computing is a prerequisite for providing customers with the services they expect in 2020. Banks and regulators need to work closely together to address the requirements for both security, competition and competitiveness.

Physical data centres and other physical IT infrastructure represent are costly, inefficient and often redundant: Since they need to be scaled for peak demand, much capacity will remain idle for most of the year. The result: sunk investment and high maintenance costs.

In realizing this redundant capacity could be leased off to others, Amazon kicked off the cloud revolution which has swept the world of IT in during the last decade, including, to an increasing extent over the last few years, financial institutions.

For banks, in the face of new competition for the end-the benefits of cloud computing are numerous. Moving data and service into public clouds enables us to build new solutions more quickly and deploy at greater scale while reducing costs. At DNB, our P2P payments app Vipps was one of our first major venture into the public cloud in 2016. We haven't looked back since.

Cloud infrastructure allow us to source single-purpose functionality from third parties into both backend and customer-facing applications almost instantly, enabling a more agile development approach.

Third-party solutions from smallish fintech partners provide the APIs behind our PSD2 integrations, the voice authentication we are piloting in our call centres, the face recognition for our ID app and the invoice scanner in our mobile bank.

Between these specialized applications and the underlying infrastructure services, today we rely on more than 50 cloud services that allow us greater speed, flexibility and security.

This migration into the cloud does not come without risks. Having fewer companies provide a deeper stack of services inevitably means concentration risks, which regulators are increasingly focusing on. Lock-in effects pose real risks to competition and vendor diversity.

> *Regulators, cloud providers and financial institutions need to work closely together ...*

Regulatory authorities are right to be vigilant about these new risks. DNB have maintained a close dialog with our chief regulators, the Norwegian FSA and the Bank of Norway. Our thinking has evolved on both sides of the table as we have gained more experience with the upsides and possible downsides of outsourcing systems of varying degrees of criticality.

Fortunately, thinking has evolved among the cloud providers we work with, too. Thanks to close dialogue with our national regulators and some of the major U.S.-based service providers, we have secured a greater degree of transparency and audit rights than seemed possible a few years ago.

Cloud providers that barely had a national presence in many EU countries, are engaging with both clients and regulators in Europe, and display a better understanding of European concerns about issues such as privacy, competition and security.

Certification and licensing regimes might be useful in certain scenarios, but current rules e.g. for payment providers means licensing regimes are already in place. Taking a risk-based approach, regulators should focus on the main platforms than entail systemic risk, as well as those that provide core financial services.

Applying stringent licensing requirements for all suppliers means erecting barriers to entry for new actors as well as many of our current providers, many of whom are precisely the kind of small, tech-savvy start-ups we should be encouraging.

In seeking to mitigate the risks of the cloud through regulatory measures, EU legislators and regulators need to be careful not to throw the baby out with the bath water. Regulators, cloud providers and financial institutions need to work closely together to ensure the European financial industry is able benefit from the power of the cloud. ●

Slaven Smojver

Director, Information Systems Supervision Department, Croatian National Bank

Use of cloud services: opportunities are clear but challenges still abound

Cloud services undoubtedly offer numerous opportunities to financial institutions. Some of the more important ones are greater efficiency in cost management, flexibility in the provisioning of computing resources and the ability to use modern technology stacks. However, the financial institutions' perception of risks related to the use of cloud services and regulatory scrutiny have stymied wider adoption.

Croatian banks have taken a cautious approach toward implementing cloud services and until now have primarily focused on the collaboration and support tools. The complexity of the cloud service providers' (CSPs) infrastructure, long supply chains and the opaqueness of their internal control mechanisms have made risk assessments quite challenging, particularly in relation to the regulatory requirements.

Recognition that small errors in the configuration of cloud environments can have an outsized negative effect (e.g. public disclosure of personal and financial data), uneasiness about CSPs' use of client's data and the need for new threat models also negatively influence information security assessments. Information asymmetry and differences in size between the dominant CSPs and their smaller clients (such as Croatian banks) further exacerbate challenges for risk assessment and relationship management.

The European Banking Authority (EBA) has defined regulatory expectations related to the use of cloud services in the banking sector in the Recommendations on outsourcing to cloud service providers and Guidelines on outsourcing arrangements. These documents recognize the use of cloud services as outsourcing. Major CSPs have recently enabled the addition of financial services addendums to their standard contracts that, as they claim, fulfil regulatory expectations. However, hurdles in the exercise of audit rights, vagueness of the shared responsibility model and uneasiness about vendor lock-in and geopolitical risks still impede a wider adoption of cloud services.

> *The financial institutions' perception of risks related to the use of cloud services and regulatory scrutiny have stymied wider adoption.*

Various developments that might mitigate some of the risks are under way. The European Commission's FinTech Action plan recognizes the need for the development of standard contractual clauses for cloud outsourcing. These would alleviate some of the issues but require further development. The initiatives such as the Gaia-X Project might reduce vendor lock-in and geopolitical risks but are still in the early phases of development.

The EBA's Guidelines on outsourcing arrangements mandate that institutions should provide competent authorities with a register of all outsourcing arrangements, which – in turn – might enable the identification of systemic risks. It is reasonable to assume that a well-thought-out framework for independent, standardized, continuous and in-depth assessment of the adequacy of CSPs control environments and the related certification and accreditation regimes would go a long way in mitigating many of the identified risks and challenges. ●

Alban Schmutz

VP Strategic Development & Public Affairs of OVHcloud and Chairman of CISPE - Cloud Infrastructure Service Providers in Europe

Towards a European framework on cloud for financial services

Banks are essential to our economies. Indeed, their continued strength together with the sovereignty of our financial infrastructures are essential for Europe's success. Who controls IT infrastructure today has become a major geostrategic question. At the same time, for the financial sector it has become key to have the ability to use massively the cloud to take advantage of greater efficiency, innovation and competitiveness.

Ongoing discussions on technological sovereignty over 5G infrastructures or on more localised production of pharmaceuticals, exacerbated by the Covid-19 emergency, remind us that the ability to control our critical infrastructure and supply chains is vital for the EU and our future.

This is why a Europe-wide framework applicable in all Member States ▶

▶ is essential. This should first deal with the reversibility and portability of infrastructure and applications to allow a rapid change of provider and easy data portability. The freedom of the financial sector to leave cloud providers quickly and seamlessly, without harming production constraints, is a key element of this sovereignty.

Second, a European framework on cloud for financial services should encompass and make explicit the necessary privacy requirement under the GDPR, particular transparency in data storage and processing locations, to ensure we are working through shared European values.

Third, such a framework has to be future proof, ideally anticipating upcoming legislation of relevance, such as the EU's Revised Payment Services Directive and other European laws that affect the ability of the financial sector to develop new value-added services that benefit companies and citizens alike. For this to succeed, a collective effort and broad public consultation is necessary.

> *Designing a robust time-to-market solution to deliver that new framework is of the utmost importance.*

The association of Cloud Infrastructure Service Providers in Europe (CISPE) is already engaging beyond financial services with European and Member State authorities to address the above challenges and to create the right environment to support businesses and customers. For example, CISPE co-chaired, together with the European association of CIOs (EuroCIO), the Working Group on a Reversibility Code for Cloud infrastructure services, which the European Commission facilitated.

Since the financial sector is a regulated sector, co-ordinated efforts between cloud service providers, European banks and EU authorities are paramount to identify the right regulatory framework. This will, in turn, foster the much-needed developments in the cloud industry, AI and other enabling technologies that are required as we move forward.

Designing a robust time-to-market solution to deliver that new framework is of the utmost importance. This is why setting up a round table between cloud service providers and European banks in close co-operation with EU authorities is very much needed to underpin the financial industry's resilience and enhance the growth potential of European economies. ●