Lending Transformation in the Cloud

Why Now, and How to Get There

By: Gareth Lewis & Piercarlo Gera

Table of Contents

Executive Summary

Foreword by Piercarlo Gera – The Digital Banking Shake-out

A Mandate for Moving Banking Processes to the Cloud by Gareth Lewis

1. Why are FIs Adopting Cloud-based Platforms?

2. How to Get a Cloud Programme Established

3. Specific Regulatory Requirements for Cloud

Conclusion

Lending Transformation in the Cloud

Why Now, and How to Get There

By: Gareth Lewis & Piercarlo Gera

EXECUTIVE SUMMARY

Adopting the Cloud is no longer a nice-to-have option for Financial Institutions (FIs) that want to lead by example; it is a requirement. The benefits offered by cloud-based platforms make them an essential solution for any bank aiming to offer a best in class product to its customers.

This white paper provides an introduction to the key drivers shaping the digital banking landscape and outlines the unique opportunity for FIs to revolutionise their value proposition by capitalising on the cloud. As with all revolutions, changes are required in order to achieve the most effective outcome, namely (i) the way people work, (ii) the integration of new systems with existing platforms, (iii) an upgrade of risk and control mechanisms, (iv) buy-in from senior management, and (v) regulatory approvals. Banks should be aiming to embrace such changes, as the benefits by far outweigh the short-term challenges. Resilience, rich functionality, speed-to-market, and scalability are the key functional benefits of the cloud, coupled with the financial and human resource benefits. As such even the regulators have focused on the use of cloud and more specifically on the areas of critical functions, audit rights and reporting, business continuity, exit and resolution plans and concentration risk. Regulatory bodies have also initiated the adoption of the cloud having evidenced its benefits and therefore will be moving the industry towards solutions which allow them to effectively regulate and enhance transparency across the financial services sector.

FOREWORD BY PIERCARLO GERA
THE DIGITAL BANKING SHAKE-OUT

The financial services market in Europe today finds itself facing an increasing number of headwinds, ranging from low growth rates across developed countries, to a low - or negative - interest rate environment impacting profitability and low price/earnings ratios. Scrutiny from regulators around capital adequacy, exposures and new reporting requirements have also dominated C-Suite attention.

For many financial institutions (FIs), digital transformation programmes have not delivered the expected outcomes. Customer experience remains poor and surveys show clients are dissatisfied by inconsistent and high effort interactions, which lag behind their streamlined experiences with Big Tech. Open banking and new entrants offering niche solutions bring further optionality to customers and serve to compound the problem for incumbents. These new players exploit the benefits of modern cloud-based technologies and are able to adapt to market and customer demands much faster than organisations tied to legacy technologies, which whilst fully amortised, are slow and expensive to change and maintain and offer little scope for innovation.

Finally, COVID-19 has become the catalysing force for FIs to prioritise digital transformation for both internal business continuity, and for customer support and engagement:

- Governments across Europe launched stimulus packages supporting local businesses and employees during the economic slowdown. Critical to the business support are government guarantees for lending which require simplified processes and online application submission, requiring FIs to rethink their processes, from applications through to underwriting and approvals,

with minimal paper and manual intervention to provide faster approvals and funding times.

- In addition to revising lending processes and rethinking customer support for the government programmes, FIs have had to transition to remote and flexible working as distancing measures were enacted to various extents across Europe. Coupled with the above government initiatives, the need for remote business planning is removing any pockets of digital resistance remaining within FIs and accelerating a digital culture revolution.

The above drivers mean FIs must act now - either by choice or for survival - and to put long-discussed digital strategies into action. A banking industry shake-out due to digital has been long suspected but not yet realised, however the current climate has highlighted the differences between those that are, and those that are not, digitally enabled. Incumbent players around the world have also proven their ability to successfully implement these digital initiatives with examples like DBS and Ping An in Asia, JP Morgan in the US, and BBVA, Santander and ING in Europe. Key to their success has been a clear business vision and digital culture backed up by having a digital talent programme in place with an appetite for, and focus on, renewing their technical architecture.

Although the future is unpredictable, as COVID-19 has shown, what is beginning to emerge is an industry structure across FIs that is shifting from an "All Winner" environment of dominant incumbents owning the market, to a highly diversified one comprising of the following segments:

Future Winners

these players are the incumbents that are evolving their `business model and becoming platforms, competing based on their relevance and brand, and leveraging technology and digital partnerships to enable this.

Utility Players

these organisations provide core banking services and have an optimised cost structure.

Losing Players

these organisations will be acquired or fail over the next three to five years.

New Entrants

these are the new challengers to the market that are digitally enabled and have the technology and ability to be nimble.

Vertical Specialists

these are focused on a specific business, for example asset managers or Big Tech organisations that specialise on payments.

Of particular interest for this white paper are the Future Winners. These incumbent organisations, facing complex technology architectures, are taking bold steps to be positioned for success into the future through business model evolution and a strong leadership team to meet changing customer needs. These FIs are able to leverage their strengths around:

- A strong customer base and brand awareness;
- Wealth of actionable data and trust from customers to manage this data;
- Risk management and risk profiling;
- Ability to blend the branch and digital for convenient and consistent customer engagement across all channels.

These Future Winners are also pursuing "volume strategies", providing their customers with more than just financial services. In a house purchase they are not simply providing a mortgage or insurance products, but also assisting with real estate services, furniture sourcing, and utilities discounts, for example. This approach also provides these FIs with multiple interaction points with their customers across a variety of channels resulting in more data consent and insights that they are able to gather to further understand and service their customers.

Successful execution of a volume strategy will often incorporate optimisation of core businesses and provide

greater personalisation of real-time marketing and lending processes which will need to be provided cost-effectively. Partnerships with additional industry players to provide a full experience on a single platform like the house-buying example above, will need to be established, in addition to establishing relationships to support Banking-as-a-Service initiatives. These provide lending or payments services, amongst others, to platforms like Amazon or Uber, for example.

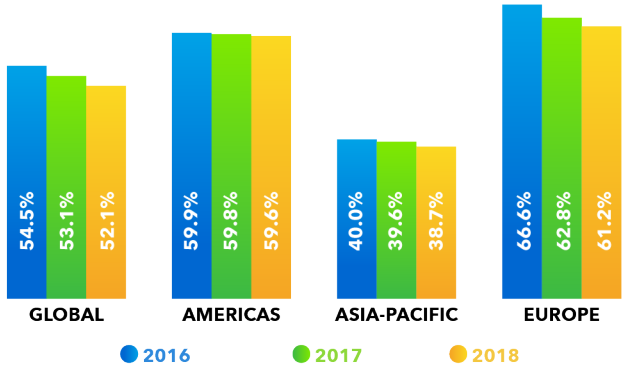
Successful execution of volume strategies and becoming a Future Winner requires a focus on digital capability development and investment. Without the right amount of digital skills and talent within an organisation, digital transformation programmes have stalled and often failed when FIs were unable to attract and retain the architects, data scientists, UX designers and AI capabilities they needed. In addition, there is a challenge to blend this talent with traditional banking talent.

Cloud and cloud-native technology is an imperative to success, providing both cost-effective ways to deploy new solutions but also enabling agility and innovation to meet the increasing speed at which customer expectations, competition, and regulatory reporting demands evolve.

With the appropriate application of cloud technology, a financial institution can solve the above challenges by:

- Reducing the cost of KYC, AML and onboarding processes
- Improving the customer and employee experience
- Increasing the speed of decision-making
- Providing more data access, control and insights
- Creating more opportunities to innovate in products and services
- Removing the burdens of regulatory reporting and changes
- Eliminating or minimising costs of maintaining and upgrading legacy on-premise technology

Those that can effectively execute on a digital strategy through the right talent, focus, and adoption of cloud will experience significant rewards. Transformation programmes can provide these Future Winners with the ability to improve cost to income ratios of below the global average of 51.2% and the European average of 61.2% to secure market share and to differentiate through personalised services, transparent and accelerated processes, and a simplified architecture built to protect against the uncertainties the future will bring.



Source: EY, Jan Bellens and Karl Meekings [1]

The remainder of this paper will explore what public cloud means for FIs in Europe, including the benefits and considerations for making the journey, how to prepare an organisation and stakeholders for such a step, and some of the key regulatory requirements.

A Mandate for Moving Banking Processes to the Cloud by Gareth Lewis

As FIs seek to address the customer demands and market dynamics as highlighted in the Foreword, a shift to the cloud is an established strategy. The need for the constant innovation that cloud technologies enable is highlighted by BBVA:

> *"Financial business models are changing to address customer demands; and the only way to change these models is through innovation."*
>
> **- Santiago Alarcón, Head of Public Cloud Strategy at BBVA** [2]

Whilst the Group Executive Chairman of Banco Santander cites new technology as a driver of opportunity and the bank's market leadership for the next decade:

"Technology is changing banking as we know it, so we are getting Banco Santander ready to make the most of the enormous strengths we have within the Group, such as technology, talent and size. This will help us make the most of the opportunities brought to us by digital innovation and become digital leaders in the financial sector over the next decade," - Ana Botin, Santander Group Executive Chairman[3].

The benefits of abandoning legacy applications and pursuing a strategy of technology renewal are proven by the likes of Santander UK[4] who have implemented such a programme in 2019, and delivered the following benefits in 2020:

- Market-leading cycle times in time-to-credit-risk-decision and time-to-cash delivery
- Reductions in manual effort of over 70% of processing time in several major tasks involved in the end-to-end lending sequence
- More flexibility in underwriting processes, providing significant digital efficiency and a more pragmatic approach
- Single customer view provided in CRM, credit risk, and product exposure systems

1. Why are FIs Adopting Cloud-based Platforms?

It may be useful to identify the three main forms of Public Cloud Services before looking at their advantages:

IAAS[5] INFRASTRUCTURE AS A SERVICE
PAAS PLATFORM AS A SERVICE
SAAS SOFTWARE AS A SERVICE

This paper will focus on SaaS, which in the context of banking could also be referred to as "Banking as a Service." The benefits of a move to public cloud are not limited to the technology and may include significant financial benefits in terms of better alignment and transparency of spend. Employment value proposition is also improved with an opportunity to develop a current and valuable skill set that legacy technology does not represent.

Functional Benefits:

- **Scale and Elasticity**
  Start small, and scale as fast as is needed.
- **Agility and flexibility**
  Use capabilities as required, and if they are not needed, then switch them off. Older in house developed applications, whilst cost effective to run, are often inflexible and cost of change is often prohibitive to the business.
- **Speed to market**
  quick to implement and deliver value.
- **Functionally rich**
  with ongoing improvements developed through direct requests from existing customers – these platforms typically have more functionality than most customers ever use and are significantly more feature rich than in house developed applications.
- **Highly Resilient**
  Cloud-based platforms are able to use the latest technologies to provide resilience far beyond that typically provided in 'active – active' dual in-house data centre architectures. Whilst it often depends on the detail of the application configuration, the basic capability is provided to fail over seamlessly between multiple sites without degradation of service.

Financial Benefits:

- **Charged to the revenue line on accounts**
  no more lumpy capital investment.
- **Variable cost**
  costs aligned with use and hence value.

People Benefits:

- By removing lower value 'infrastructure' tasks, staff are free to work on higher value activities core to the business and service innovation.
- Staff get to work with the latest technologies, which builds a current and valuable skill set and improves the employment value proposition and staff retention as a result.
- Reduced reliance on hard to find resources to support and develop legacy applications.

2. How to Get a Cloud Programme Established

In order to capture the very substantial benefits of a cloud platform, a number of changes are required covering the way people work, integrations with existing platforms, an upgrade of risk and control mechanisms, gaining buy in from senior management, and regulatory approvals. Whilst these are very real challenges, none are insurmountable, and the business benefits far outweigh the pain of the change.

Initial Steps – How Do Most FIs Get Started?

Initial usage of cloud platforms typically starts with some developments on in-house cloud platforms, some usage of SaaS applications, and some experiments with IaaS providers.

Private cloud is certainly being used by many companies today and is characterised by virtualisation of the infrastructure through the use of a hypervisor[6]. Whilst a useful initial step, it does not bring the full benefits of full-blown cloud strategies, and many companies rapidly supplement with further developments.

The next steps typically include the use of IaaS as a vehicle for both developing and testing in-house or outsourced code developments. This is low risk and yields major benefits for many FIs. This is often followed by the use of IaaS platforms and their associated tooling to provide storage for data, and analytics capabilities. The ability to scale up and down activity being the prime benefit in this application.

Further steps then include the expanded use of SaaS platforms.

Early cloud adopters tended to favour non-mission critical applications such as HR platforms, however, the real benefits occur where the SaaS platforms are used for activities that are more central to the business, such as radically improving the client or colleague experience.

Examples include customer relationship management (CRM) solutions or platforms that make client onboarding or product origination a frictionless experience for clients, colleagues, and intermediaries alike by automating and streamlining middle- and back office processes.

In the full-blown implementation of cloud-first strategies, the most advanced companies are deploying multiple approaches:

1. Developing new applications to run on cloud
2. Using SaaS providers to provide specific leading-edge functionality; and
3. Refactoring their existing applications to take advantage of cloud infrastructures.

Key Challenges and How They are Addressed

In order to capture the benefits of using the cloud a series of changes and challenges need to be addressed. The key ones are:

- Ensuring that the Main or Supervisory Board and the Regulators are comfortable with embarking on a journey of significant strategic change through an effective governance process.
- Adapting the way in which change is delivered in the firm to embrace the use of cloud and ensuring that it is both integrated during, and supportable after, implementation.
- Ensuring that the way in which cloud is adopted remains within the risk profile of the firm for all aspects, particularly security and resilience.

These high-level considerations break down into the following topics which will be investigated further in this paper:

- Main Board Responsibilities
- Cloud Compatible Governance
- Risk and Control Frameworks
- Target Operating Model
- Supplier Contracts
- Data Residency, Transit, Storage, Processing and Access Controls
- Security
- Multi Cloud Support and Service Management
- Network
- Economic Drivers for Cloud

Main Board Responsibilities

In what may ultimately be a significant strategic change to the way in which a business operates, the main or supervisory board must be fully cognisant of the implications of embarking on such a path. Indeed, the regulatory authorities will insist that they are both informed and comfortable with the risk and benefit trades that are inherent in this change.

Central to the discussion will be the Chief Risk Officer, whose role is to assure board members that the risk profile of the firm remains within the acceptable limits that have previously been agreed by main board officers.

These risks would primarily be operational risks triggered by failure scenarios such as data breach, and system failure or outage. They apply not only to cloud activity but any and all activities within the firm. Failure to address these effectively could potentially result in customer impact, financial loss, brand damage or regulatory censure over an extended period of time.

It is critical therefore, that the main board, executives, and others who have risk management responsibilities or may be contacted by regulators are kept fully informed through appropriate governance mechanisms.

Governance

Key to the delivery of any programme of work is the ability to govern the changes in an appropriate manner. A cloud-based programme is not dissimilar to many implementations but given the cross-business nature of most cloud programmes, it is critically important that any governance structure established is effective. Appropriate governance and risk management are usually the first discussions with any regulator, and therefore need to be both effective and evidenced from the beginning.

Risk and Controls Frameworks

The primary mechanism for the exercise of oversight by the regulator is through the examination of the effectiveness of the risk and control functions of the FI. Whilst these are often well understood for existing (often in-house) business services, they are less well formed for any services that are outsourced to SaaS providers or other third parties. Regulators are increasing focus in this area and require FIs to satisfy themselves of the effectiveness not only of their own risk and controls but also those of the third-party outsourcer. It is critical to develop this framework and test third parties at the beginning of any contract. The regulations require that this is done at regular intervals to ensure that the service provided remains within tolerance levels and that controls remain effective.

Target Operating Model

The ability to switch on and off compute capability will allow business functions to perform tasks previously unthinkable. The operating model of the firm will need to change in order to obtain the most benefit from a cloud implementation. Whilst this catalyses business innovation, which in turn results in the opportunity to restructure the business, the supporting Information Services functions will also need to change in significant ways. Typically, this occurs over a few iterations, as cloud adoption moves from start up to mainstream, and is integrated with more agile ways of working.

Application developers and integrators will be freed up to develop and deploy new applications rapidly, and infrastructure architects used to build data centres will need to be retrained in cloud configuration activities. Security and other control functions will also need to embrace new ways of working with the cloud-based systems.

Supplier Contracts

Typical supplier relationships with outsourcing partners, software and hardware vendors will change significantly. Established 'traditional' vendors find that hardware and software upfront licence fees will disappear to be replaced by cloud offerings with utility-based subscriptions based on usage. The new cloud relationships will be revenue based and longer term in nature. Once the journey to cloud has been established (whether SaaS, IaaS or other), it is very rare that the service is brought back in house. The terms of the contract will be markedly different from those currently used, with little or no negotiation on certain terms.

SaaS providers typically prefer contracting based on module functionality and have deliberately architected the application to be modular and with other common applications through APIs to allow seamless creation of the enterprise architecture.

Data Residency, Transit, Storage, Processing and Access Controls

The question of data management is already a hot topic in most FIs, and few have really managed the challenge well. The adoption of cloud platforms does not solve this issue. In fact, without proper management, data can be further

fragmented and dispersed across the enterprise and cloud. However, a move to the Cloud is a great opportunity to ensure that data is cleaned, validated, and migrated to the new system, and hence obtain greater control than before when implementing a new platform.

The control of a FI or nation's data is a critical question that requires careful consideration. Cloud platforms may offer the ability to seamlessly move both applications and data around the world as the workload varies by geography and time of day. Of course, it is possible to restrict this through technical and legal measures to more local cloud centres (for example, to keep data processing within the EU), however there still can be residual concerns over the cloud security of the data, for example when it comes to US or Chinese owned and headquartered firms. The US has gone some way to alleviating this through the implementation of the Cloud Act, the judicious use of encryption keys, and other measures provided by the FI (rather than sole reliance on those of the cloud provider) allows further levels of protection[7].

More than 80 countries have now determined that the data pertaining to its citizens will need to remain resident in country, although data which has an international dimension, for example, UK financial data for a US corporation, would not be subject to this. Additionally, there are concerns over which countries are transited as data moves between cloud data centres, and this too needs consideration. In summary, there is a need to carefully manage the process of data storage in cloud to ensure that it conforms to all local and international rules on data use and storage. In Europe this is covered by adherence to GDPR[8].

Security

Security is another key area of concern although it could be argued unfounded as the public cloud suppliers are fully aware that confidence in their services are based on faultless security[9]. By choosing a solution built on a widely adopted platform like Salesforce, FIs are tapping into a highly trusted provider[10]. Security of cloud-based platforms should be considered at two specific levels. Firstly, security OF the cloud itself. Secondly, security IN the cloud of data and applications.

OF the cloud refers to the physical infrastructure of the cloud datacentre, and associated hardware and software to operate. It is the responsibility of the cloud provider, and the security offered is typically significantly stronger than most firms' data centres. As an example, most cloud providers offer full encryption of data at rest and in transit. In most FIs data centres, the data is unencrypted.

The security IN the cloud refers to the applications and data that may run on a cloud infrastructure. In the case of SaaS, the responsibility lies primarily with the provider, although who and how a FI uses the data is determined by admin and access privileges that the FI will need to configure.

Source: Amazon, "Shared Responsibility Model", https://aws.amazon.com/compliance/shared-responsibility-model/

If further assurance is required over the control of a FI's data, it is possible to access to the data through the use of user owned and managed encryption keys for the encrypted data. In extreme cases, it is possible to segregate the data into FI owned or managed data centres and perform one or a combination of the following (a) re-integrate at the point of use, (b) tokenise key information or (c) mask the data itself. For the vast majority of use cases, these measures are not required.

To ensure the safety of client data, cloud providers rely on skilled cyber security teams backed by the latest security technologies - resources that are often well beyond what their customer organisations could afford on their own. Effective cloud providers offer security solutions at every security level, including infrastructure security, network security, and application security, to counter threats both internal and external.

Cloud providers also bring with them the added security of compliance. Especially among regulated industries, the issue of compliance is one that plays an important role. Cloud platforms can be designed to include compliance tools, constantly updated to reflect ongoing changes to regulatory laws. This protects businesses in ways that would be difficult to emulate with basic in-house solutions.

As a widely adopted public cloud provider trusted by over 150,000 businesses globally to safeguard their data, Salesforce is an example of a provider committed to achieving and maintaining trust and security and providing a robust compliance program[11]. Choosing a cloud solution built on a platform such as Salesforce provides greater security, control and data protection than an individual FI could implement and enforce on its own.

Multi Cloud Support and Service Management

Moving to employ multiple clouds, which most enterprises will settle on as a model for enterprise operation, requires that these are capable of being supported and managed effectively. Use of a SaaS service effectively alleviates the majority of the work from the existing support teams, as both infrastructure and the application are now the responsibility of the SaaS provider, and hence are automatically upgraded as part of the service. There does, however, remain a role for the central support team in managing resolution of any issues in using the SaaS provider. There is also a role in ensuring that integration between applications, whether cloud or firm based, continues to work effectively as newer releases of applications are deployed. As SaaS interfaces are always forward compatible, the support and service management roles become more integration focused rather than application focused.

Network

As cloud-based applications grow, but the core of the business remains within pre-existing data centres, it will be necessary to upgrade network infrastructure linking the sites. Whilst a significant increase in bandwidth is likely to be required, the use of 'Co-location' centres - where all major cloud and telecoms providers are interconnected - means that the interconnection question is relatively straightforward. There remains, as ever, the question of upgrading end user sites connectivity to the SaaS or other cloud platforms directly. This does not always require significant increases as the application may be replacing existing in-house applications, and modern architectures can be 'less chatty' than existing older technologies.

Economic Drivers for Cloud

The question of whether the cloud is more expensive than an on-premise implementation is a common one for executives. The answer, of course depends on a range of factors:

- The speed with which new ideas can be brought to market. This speed to value is typically undervalued in most organisations.
- The capability of the existing in-house application – is it fit for purpose and delivering business value?
- The nature and performance of the people applied to operating existing platforms. Are they in-house, outsourced, or contracted?
- The nature of the application. Is it used permanently at a steady rate, or are there peak workload periods which determine the systems dimensions?
- The current situation regarding hardware and software refresh cycles, and in particular contractual obligations for data centre re-contracting.

There is not a predetermined answer, but in general, most firms are obtaining enormous business value through the use of cloud computing, and in many cases proving the investment to be more than worthwhile. New entrants and disruptors go one step further using cloud as a core enabler of that disruption.

3. Specific Regulatory Requirements for Cloud

Regulation has been a dominant feature of banking executives' lives for several decades now, with a steep increase in focus since the 2008 crisis. Often seen as an ever-increasing burden, the regulators have turned their focus to operational resilience and the use of cloud specifically. The key question that executives therefore often have is the position that both the in-country and 'host' regulator[12] have concerning cloud adoption.

Whilst this is a developing area, the US, Singapore, Hong Kong, UK and a number of other countries have forged ahead on cloud adoption, and FIs have adopted its use at scale. In Europe, the UK was the first country to issue cloud guidelines in 2014, with updates in 2016 and most recently in September 2019. The European Commission has also published guidance in the European Banking Authority Guidelines (EBA[13]) Cloud Recommendations now embodied in the EBA Outsourcing arrangement to be applied from September 2019. These are a minimum set of recommendations for Europe, and individual country regulators may have a desire to further extend these recommendations. In relation to cloud, these consist of the following key areas:

- **Critical or Important Functions**
  FIs must assess the 'materiality' of the workload to be outsourced, based on legal, reputational, financial and customer impacts should the service fail. The definition of materiality is at the discretion of the executive of the organisation, but typically has parameters such as duration of outage, number of customers affected, financial and reputational impact tolerances. etc.

- **Audit Rights and Reporting**
  EBA rules require FIs to be able to audit the CSPs[14] , and many have now welcomed this and provide excellent auditability. This has now largely been embodied in normal CSP master contracts, and FIs may avail themselves of audit rights should this be required.

  EBA rules also require that firms report cloud workloads on a regular basis, including SaaS, PaaS and IaaS. Reporting takes place to the host regulator, who then remits the data to the EBA.

- **Business Continuity, Exit and Resolution Plans**
  Whilst regulatory scrutiny on Business Continuity Planning / Disaster Recovery (BCP/DR) plans have been in evidence for some time, regulators have announced the intention to further scrutinise digital and cloud-based platforms through an operational resilience lens. This includes the need for well thought through exit plans should the provider fail either technically of commercially. Whilst there is less concern over 'noncritical functions', there is a clear concern over the ability of a firm to survive failure of systems supporting 'critical functions'.

  There is also an increased awareness that overburdened legacy systems can be at the heart of issues, and regulators are well attuned to FIs' management avoiding the upgrade or replacement of systems due to the risk of change.

  In summary, with careful architecting, SaaS and other applications can meet regulatory requirements, and there is an expectation that often fragile legacy platforms will need to be significantly upgraded and changed to support new market offerings.

- **Concentration Risk**
  Finally, regulators are carefully monitoring the implications of multiple workloads in a single FI and multiple FIs' use of cloud providers with a focus on the concentration risk that is possible given the wholesale move to cloud. Whilst this is not an issue today, there is concern in the 3-5-year horizon that this could be of concern.

- **Regulators' Own Use of the Cloud**
  Whilst regulators may have concerns over cloud usage, it is clear that they themselves have increasing reliance on the capability to perform their role. Both Financial Industry Regulatory Authority (FINRA[15]) in the USA and the FCA[16] in the UK have been pioneers in the use of cloud-based technologies and have been extensively using many cloud-based platforms since 2014. In the case of the FCA these include Salesforce, Amazon, Oracle and others. In the case of FINRA, the use of Amazon Web Services allows them to process, on average 67 billion transactions a day, which would otherwise not be possible on normal data centre-based technologies.

  Both these regulators hold sensitive information for the whole industry and have satisfied themselves of the security and resilience requirements fundamental to protecting firm and industry data.

  It should be further noted that the European Commission[17], and banking trade associations such as the EBF[18] are very supportive of the use of cloud-based infrastructure and have a number of active working groups to further advance and simplify the use of cloud in Europe. There is, in addition, a Cloud Code of Conduct[19] that sets out certification requirements and has been adopted by a number of cloud leaders as a mechanism of assurance of compliance to a variety of standards.

As Wim Mijs, CEO of the EBF says: "Cloud is the foundation of a competitive Digital Single Market for Europe.

> *All the banks participating in this project believe that cloud computing is the only way to transform into agile and globally competitive organisations.*

The Cloud Banking Forum has aligned bank supervisors' expectations and cloud providers' offerings and I am glad it is echoed by the sector pushing cloud adoption upwards[20]."

CONCLUSION

FIs have an opportunity to revolutionise their market offerings in terms of speed-to-market and flexibility using the cloud. New business models can be tested, proven and evolved in a manner simply not possible using legacy technologies.

Those able to effectively execute on a digital strategy through the right talent, focus, and adoption of cloud will be the winners in the long term and prosper in the new age of banking. Those that hesitate may find they face even stronger headwinds in the future with potentially fatal consequences.

There is widespread evidence that the use of cloud computing in all its forms brings enormous advantages to those who chose to adopt the capability. Many new market entrants, as well as existing FIs, have made the leap to embrace the cloud and are already enjoying the benefits that it brings.

ABOUT THE AUTHORS

Gareth Lewis

Gareth is an independent consultant with a focus on Digital Transformation primarily in the domains of Financial Services and Telecommunications. Gareth has held a number of senior technology leadership roles in his career, including serving as CIO of the Financial Conduct Authority (FCA) in the UK, Group CIO for Centrica, a FTSE 30 company, Group CIO for Virgin, as well as being a Partner at KPMG. Gareth has also spent a number of years on the AWS Global advisory board, and recently advised the UK Government Treasury Committee on how to regulate Operational Risk in the Financial Services sector. Prior to this he was at the heart of the Global Cloud Programme for HSBC.

Piercarlo Gera

Piercarlo is the CEO of Gera & Partners, operating as a Senior Advisor and Advisory Board Member of Private Equity Firms and Companies, with a focus on Digital Strategy and Digital Transformation, with a particular focus on the Financial Services sector. Until October 2019 he was the Senior Managing Director at Accenture, where he started his career and in the last 20 years had various global business responsibilities. Piercarlo has been listed among the Top 50 Digital experts globally by "Digital Banking Power 50" and has been the author of several leading-edge articles and publications on financial services, platform economies, and revenue drivers for FIs.

About nCino

nCino (NASDAQ: NCNO) is the worldwide leader in cloud banking. The nCino Bank Operating System® empowers financial institutions with scalable technology to help them achieve revenue growth, greater efficiency, cost savings and regulatory compliance. In a digital-first world, nCino's single digital platform enhances the employee and client experience to enable financial institutions to more effectively onboard new clients, make loans and manage the entire loan life cycle, and open deposit and other accounts across lines of business and channels. Transforming how financial institutions operate through innovation, reputation and speed, nCino works with more than 1,100 financial institutions globally, whose assets range in size from $30 million to more than $2 trillion. For more information, visit: www.ncino.com.

ENDNOTES

[1] *EY, Jan Bellens and Karl Meekings, "Why global banking profitability will remain a challenge in 2020", Feb 2020.*

[2] *BBVA, Digital Processing, "Google Cloud helps BBVA work in a more agile and collaborative way", October 2018.*

[3] *Santander, Technology, "Talent and Size to underpin Santander's Strategy", April 2019.*

[4] *Celent Case Study: Santander UK, "Santander UK Wins Celent Model Bank Award for Commercial Lending in Partnership With nCino", April 2020.*

[5] *Infrastructure as a Service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet. It is one of the three types of cloud services, along with software as a service (SaaS), and platform as a service (PaaS). Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. PaaS is IaaS plus useful tools often for development purposes such as database, middleware and simple analytics services.*

[6] *Hypervisor is computer software, firmware or hardware that creates and runs virtual machines.*

[7] *Cloud Act, "Clarifying Lawful Overseas Use of Data act", 2017-2018.*

[8] *GDPR: General Data Protection Regulation. Regulation specific to privacy and protection of data in the EU. It also applies to transfer of personal data outside the EU.*

[9] *Salesforce, Customer 360 Platform, "Silver Linings: Why Your Data Is Safer in the Cloud".*

[10] *Further information about Salesforce and security can be found here: https://trust.salesforce.com/en/*

[11] *Salesforce Trust Home: https://trust.salesforce.com/en/*

[12] *Host regulator: the country where the firm has its HQ acts a s the host regulator, and authorisations are obtained through this route. These can be 'passported' to other jurisdictions.*

[13] *European Banking Authority Guidelines on Outsourcing Arrangements, October 2019, further guidelines have been issued by other authorities.*

[14] *CSP: Cloud service providers such as Salesforce, Microsoft Azure, Amazon Web Services or Google.*

[15] *FINRA: Financial Industry Regulatory Authority. Itself regulated by the US Government Securities and Exchange Commission. A non-governmental organization that regulates member brokerage firms and exchange markets*

[16] *FCA: Financial Conduct Authority. UK Conduct regulator, which in turn provides services to the Prudential Regulation Authority at the Bank of England.*

[17] *European Cloud Strategy 2012.*

[18] *European Banking Federation, Cloud Adoption by European Banks.*

[19] *EU Cloud Code of Conduct, "Your Path to Trusted Cloud Services in Europe".*

[20] *EBF Press Release, "Two Years on: EBF Cloud Banking Forum".*