Financial services in a post-pandemic world: How cloud-based intelligent enterprises will forge the path ahead

Received (in revised form): 25th May, 2021

Jennifer Geary
General Manager of EMEA nCino, UK

Jennifer Geary serves as nCino's General Manager, EMEA. In this role, she is responsible for nCino's full European functions, spearheading business expansion across the Continent and into Africa and the Middle East. Geary has more than 20 years of experience in finance, technology, risk and legal, across diverse industries from financial services to not-for-profit. Prior to nCino, she was the Chief Risk and Operations Officer at Asto UK, a FinTech backed by Santander. She also spent 13 years in Barclays plc, initially in investment banking, followed by wealth management and, finally, as Chief of Staff to the Group General Counsel. Jennifer holds a B.Comm from University College Dublin and a Master's in Accounting from the Michael Smurfit Graduate School of Business.

EMEA, nCino, c/o Natalia Moose, Metal Box Factory, 30 Great Guildford Street, London SE1 0HS, UK
E-mail: jennifer.geary@ncino.com

Abstract COVID-19 has shown financial institutions (FIs) globally that the ability to respond quickly to unexpected challenges and continuously innovate to meet changing customer expectations and an ever-evolving industry is vital. Those institutions utilising cloud-based and cognitive technologies will have a competitive advantage over those that avoid or resist meaningful digital transformation. This paper will explore the benefits of cloud adoption and artificial intelligence (AI) and discuss how FIs can employ these technologies to help future-proof their organisations.

KEYWORDS: SaaS, BaaS, artificial intelligence, machine learning, cognitive technologies, cloud, digital transformation, intelligent enterprise

INTRODUCTION

The financial service industry today faces more and more headwinds in the wake of COVID-19, ranging from low growth rates across developed countries, to a low or negative interest-rate environment impacting profitability and price/earnings ratios, to scrutiny from regulators around resilience, exposures and new reporting requirements. Perhaps the biggest takeaway for financial services from the global pandemic is the importance of digital transformation and need for cloud-based digital technology. When COVID-19 struck and much of the world moved to remote work, the financial institutions (FIs) that had access to tools and technologies housed in the cloud were able to continue their work without interruption. Those that did not struggle to operate their organisations, keep their employees productive and support their customers.

COVID-19 has shown FIs that the ability to respond quickly to unexpected challenges and continuously innovate to meet changing customer expectations and an ever-evolving global industry is vital. Those FIs utilising

cloud-based and cognitive technologies will have a competitive advantage over organisations that choose to resist digital transformation. This paper will explore the benefits of the cloud and artificial intelligence (AI) and discuss how FIs can employ these technologies to future-proof their organisations.

COVID-19: DIGITAL TRANSFORMATION'S CATALYST

Traditionally, FIs have relied on home-grown, on-premises technology and/or multiple, disparate systems to handle their banking operations. Such systems were built in a time of manual processes that result in redundant and duplicative data entry, thereby increasing the likelihood of human error and a poor customer experience. Information is siloed within the organisation, leading to a lack of transparency and loss of efficiency. Although many FIs had already recognised the need to update their ageing systems prior to the onset of COVID-19, the global pandemic served to significantly accelerate digital transformation within the financial services industry. Having flexible, digital technology accessible to employees and customers, regardless of location, became essential to business continuity. COVID-19's direct impacts on financial services:

- Governments across North America and Europe launched stimulus packages supporting local businesses and employees during the economic slowdown. Putting these loans into operation required simplified, high-scale processes and online application submission, forcing FIs to rethink their processes, from applications to underwriting and approvals, with minimal paper and manual intervention to provide faster approvals and funding times. Reporting on the performance of these portfolios is also critical.
- In addition to revising lending processes and rethinking customer support for the government programmes, FIs had to transition to remote and flexible working as distancing measures were enacted. Coupled with the above government initiatives, the need for remote working served to remove any pockets of digital resistance remaining within FIs and accelerated a digital revolution.

Alongside the relentless march of the challenger banks, the above drivers mean FIs must act now — either by choice or for survival — 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 who are and those who are not digitally enabled. Many incumbent players around the world have proven their ability to successfully implement these digital initiatives with examples like DBS Bank and Ping An in Asia, JP Morgan in the US and BBVA, Santander and ING in Europe. Important 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.

Current state of the industry

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 the following segments:

- **Future Winners:** These players are the incumbents that are evolving their business model and becoming platforms, competing on the basis of 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.
- **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 in payments.
- **Losing Players:** Organisations that are not clear about their place are failing to innovate and will be acquired or will fail over the next three to five years.

Of particular interest for this 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 the following:

- A strong customer base and brand awareness;
- A wealth of actionable data and trust from customers to manage this data;
- Risk management and risk profiling; and
- The ability to blend the branch and digital for convenient and consistent omnichannel customer engagement.

These Future Winners are also pursuing 'volume strategies', providing their customers with more than just financial services. 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.

Partnerships with additional industry players to provide a full experience on a single platform will need to be established in addition to establishing relationships to support white-labelled Banking-as-a-Service (BaaS) initiatives. These provide lending and payments services, among others, to platforms like Amazon or Uber, for example.

Successful execution of volume strategies and becoming a Future Winner require 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, user experience (UX) designers and AI capabilities they needed. In addition, there is a challenge to blend this talent with traditional banking cultures.

THE CASE FOR THE CLOUD

Cloud and cloud-native technology are imperative to success, providing a cost-effective way to deploy new solutions. In addition, cloud allows 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, an FI can solve the aforementioned challenges by

- Reducing the cost of know your customer (KYC), anti-money laundering (AML) and onboarding processes;
- Improving the customer and employee experience;
- Increasing the speed of decision-making;
- Providing more granular data access control and insights;
- Creating more opportunities to innovate in products and services;
- Meeting the burdens of regulatory reporting and changes; and
- Eliminating or minimising costs of maintaining and upgrading legacy on-premises technology.

The FIs 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 reduce cost to income ratios below the global average of 51.2 per cent and the European average of 61.2 per cent 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 (Figure 1).[1]

As FIs seek to address the customer demands and market dynamics, a shift to the cloud is an established mainstream 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]

Additionally, 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 moving on from legacy applications and pursuing a strategy of technology renewal are proven by the likes of Santander UK,[4] which 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;

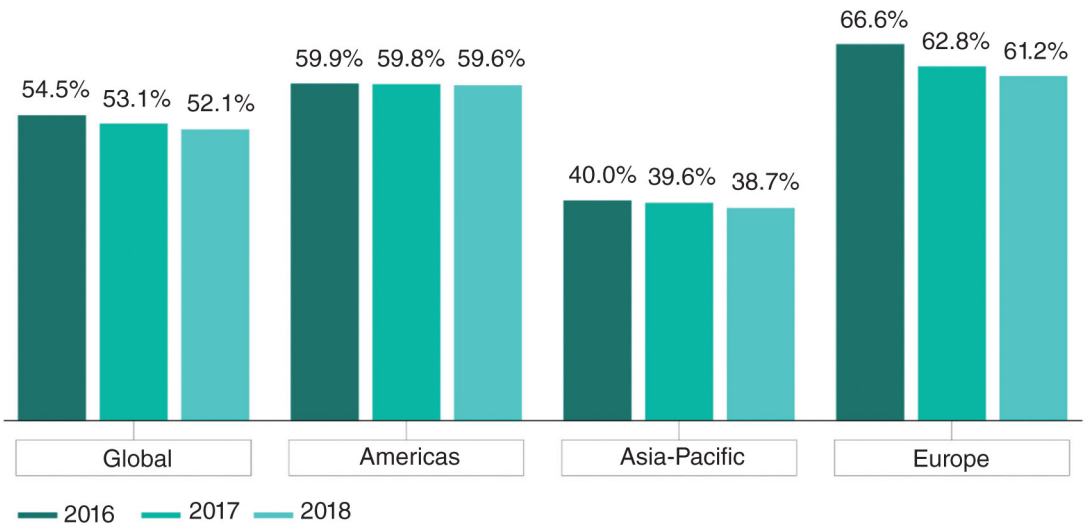

Figure 1: Average efficiency ratio by region

Note: Weighted average cost income-ratio for top global banks in terms of asset size (2018).

Source: S&P Global Market Intelligence, EY analysis.

- Reductions in manual effort of over 70 per cent 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; and
- Single customer view provided in customer relationship management (CRM), credit risk and product exposure systems.

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 of Moving to Cloud Technology:

- **Scale and Elasticity:** Organisations can start small and scale as fast as is needed.
- **Agility and flexibility:** The ability to use capabilities as required, and if they are not needed, then switch them off. Older in-house developed applications 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. While 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.
- **Security:** Cloud providers have the scale to invest in cutting-edge security and encryption, often better than individual FIs can afford to pay for themselves.

Financial Benefits:

- **Charged to the Revenue Line on Accounts:** As cloud technology is billed as a regular services, this means no more lumpy capital investment in hardware.
- **Variable Cost:** Costs are aligned with use and hence the value they deliver.

People Benefits:

- By removing basic 'infrastructure' tasks, staff are free to work on higher value activities central to the business and customer service.
- 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.

ESTABLISHING A CLOUD PROGRAMME

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. While these are very real challenges, none are insurmountable, and the business benefits far outweigh the pain of the change.

Initial usage of cloud platforms typically starts with some developments on in-house cloud platforms, some usage of SaaS (Software as a Service) applications and some experiments with IaaS (Infrastructure as a Service) 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.[5] While 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 activity up and down is 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 human resources (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 customer or employee experience. Examples include CRM solutions or platforms that make customer onboarding or product origination a frictionless experience for customers, employees 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.
3. Refactoring their existing applications to take advantage of cloud infrastructures.

ADDRESSING CHALLENGES TO THE CLOUD

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

- Ensuring that the board and regulators are comfortable with the FI 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 appetite of the firm for all aspects, particularly security and resilience.

These high-level considerations break down into the following topics, which we will investigate 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

BOARD RESPONSIBILITIES

In what may ultimately be a significant strategic change to the way in which a business operates, the board must be fully cognisant of the implications of embarking on a path to cloud technology. 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 and Chief Technology 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 the Directors.

Board concern usually centres on failure scenarios such as data breach and system

failure or outage. They apply to not only cloud activity but all other 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. It is critical, therefore, that the main board, executives and others who have risk management responsibilities or who may be contacted by regulators are kept fully informed through appropriate governance mechanisms and reassured as to the security and resilience of the solution being proposed. The irony is that the generally accepted thinking in technology circles is that cloud computing is more consistent, better managed, more homogeneous and more resilient than traditional on-premise offerings.

GOVERNANCE

Important to the delivery of any programme of work is the ability to govern the changes appropriately. A cloud-based programme is not dissimilar to many implementations, but given the cross-business nature of most cloud programmes, and the potential sensitivity of the data, it is critically important that any governance structure that is 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 CONTROL 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. Although these are often well understood for existing (often in-house) business services, they need to be amended 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 risks 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. Fortunately, frameworks for managing third-party supplier risk are now commonplace and widely available.

TARGET OPERATING MODEL

The ability to dial up and down processing 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. While this catalyses business innovation, which in turn results in an 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 early adoption 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. While there is unavoidable change, however, this is usually popular with technology staff, because these are marketable and valuable skills to learn.

SUPPLIER CONTRACTS

Typical supplier relationships with outsourcing partners and 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 linked to volume and usage and will be longer term in nature. Once the journey to cloud has been established (whether SaaS, IaaS or other), we have seen very few cases in which the service is brought back in house. The terms of the cloud contract will be markedly different from those currently used, with little or no negotiation on certain terms, in order to preserve the homogeneity of the service. This, in itself, however, can be a benefit, as it frees up time spent in tortuous negotiation to focus instead on products and services that make a difference to customers.

SaaS providers typically prefer contracting based on module functionality and have deliberately architected the application to be modular and to work 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 a hot topic in most FIs, and most struggle with this topic in some way. The adoption of cloud platforms does not solve this issue in itself. In fact, without proper management, data can be further fragmented and dispersed across the enterprise and cloud. A move to the cloud, however, is a great opportunity to ensure that data is cleaned, validated and migrated to the new platform and hence obtain greater control than before. This also helps with record retention and data classification.

The location and jurisdiction in which data is held require careful consideration. Cloud platforms may offer the ability to move both applications and data around the world because 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 (eg to keep data processing within the EU). There can still be residual concerns over the cloud security of the data, for example, when it comes to US, Swiss, Singaporean or Chinese-owned and headquartered firms. The US has gone some way towards alleviating this through the implementation of the Cloud Act, the judicious use of encryption keys and other measures that can be adopted by the FI (rather than sole reliance on those of the cloud provider) and that allow further levels of protection.[6]

More than 80 countries have now determined that the data pertaining to their citizens will need to remain resident in the country, although data that 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 through 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 the 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.[7] Cloud providers, however, are aware of this and have structured their offerings accordingly.

SECURITY

Security is another notable area of concern, although public cloud suppliers are fully aware that confidence in their services is based on faultless security.[8] By choosing a solution built on a widely adopted platform like AWS, Azure or Salesforce, FIs are tapping into a highly trusted provider.[9]

The security of cloud-based platforms should be considered at two specific levels. Firstly, security *of* the cloud itself. Second, security *in* the cloud of data and applications:

- *Of* the cloud refers to the physical infrastructure of the cloud data centre 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 256-bit advanced encryption of data at rest and in transit. In most FIs' data centres, the encryption is typically less strong.

- 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 how an FI uses the data is determined by admin and access privileges that the FI will need to configure.[10]

If further assurance is required over the control of an 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 customer data, cloud providers rely on skilled cybersecurity 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. They are also regularly and rigorously audited.

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 more than 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 programme.[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 some 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 are hence 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, if some of the core processing of the business remains within pre-existing data centres, it will be necessary to upgrade network infrastructure linking the sites. While 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 because the application may be replacing existing in-house applications, and modern architectures can be 'less chatty' than older technologies.

ECONOMIC DRIVERS FOR THE CLOUD

The question of whether the cloud is more expensive than an on-premises 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 skill set of the people tasked with 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 that determine the systems dimensions?
- The current situation regarding hardware and software refresh cycles and, in particular, contractual obligations for data centre recontracting.

There is no 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 an important enabler of that disruption. In addition, the 'agility' of spend, turning large fixed costs into monthly variables ones, allowing organisations to ramp up or down their processing power as required is an important benefit.

REGULATORY REQUIREMENTS FOR THE 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 important question that executives therefore often have is the position that both the in-country and 'host' regulator[12] have concerning cloud adoption.

While this is a developing area, the US, Singapore, Hong Kong, the 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 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 important 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 and financial and reputational impact tolerances.

- **Audit Rights and Reporting:** EBA rules require FIs to be able to audit the cloud service providers (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:** While 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 or commercially. While there is less concern over 'non-critical 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 owing to the risk of change. 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:** 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. While this is not an issue today, there is an expectation in the three to five year horizon that this could be of concern and require mitigation.
- **Regulators' Own Use of the Cloud:** While regulators may have questions over cloud usage, it is clear that they themselves have increasing reliance on the capability to perform their role. Both the Financial Industry Regulatory Authority (FINRA)[15] in the US 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. 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. The Cloud Code of Conduct[19] 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]

AGILITY AND INTELLIGENCE IN THE CLOUD

In financial services, being an agile enterprise centres on the idea of turning important banking functions — from product development and customer acquisition to account opening and commercial lending — into a systematic, fast and frictionless process. This requires a configurable and flexible system of engagement in the cloud that allows FI employees and customers to collaborate in real time, with full transparency and visibility at every step of the process. Once an FI has taken the critical step towards achieving transformative change by implementing a cloud-based solution, it begins to achieve efficiencies and agility across the organisation.

Innovation, however, is a journey, not a destination, which is why institutions that have embraced agility in the cloud must take the next step forward and become an intelligent enterprise, which means building on the benefits afforded by agility and leveraging cognitive technologies to capture deeper customer insights, make informed, data-driven decisions, reduce costs, manage risk and increase efficiencies.

AI is quickly transitioning from a 'nice-to-have' technology to an important business driver for financial services organisations. According to a 2019 World Economic Forum survey, 77 per cent of all respondents named AI as having high or very high overall importance to their businesses over the next two years.[21] FIs have begun to think about AI beyond the abstract and are discovering the many practical and profitable use cases for this technology. A growing number of FIs have started truly understanding the importance of using AI to enhance the customer and employee experience.

AI and related technologies, including machine learning, natural language processing and cognitive computing, serve as the foundation of the cloud-based intelligent enterprise. There is a broad array of current and potential use cases within financial services for AI and related technologies, ranging from robo-advice and next-product recommendations to AML compliance and credit card fraud protection.

Within the intelligent enterprise, cognitive technology can be utilised to bring a true ROI to the institution. FIs need actionable insights to maintain competitiveness and serve their customers' needs. The successful deployment of the intelligent enterprise can help increase revenue, grow profitability, improve efficiency, reduce costs and mitigate risk. One study, for example, found that FIs that invest in AI and other cognitive technologies across the enterprise could see an average revenue growth of 34 per cent.[22] Embedding cognitive technologies into core banking processes can present FIs with measurable results, a positive ROI and benefits that continue to increase over time.

CHALLENGES TO AI ADOPTION

All of this is not to say that widespread transformation to the intelligent enterprise will come easily. Incumbent FIs of all sizes come burdened with long-held processes and systems that serve as barriers to change. The industry faces a number of daunting challenges, including the burden of legacy systems, slow adoption rates, talent acquisition and competition from big tech and FinTech upstarts.

It is important to start small and focus on incorporating cognitive technologies seamlessly into existing processes while also maintaining a human touch with customers, that is, to build AI solutions that augment employees' capability and put the customer first. The most effective way to achieve this ideal is through the deployment of a single, cloud-based platform and a system that seamlessly captures and analyses data from all customer channels and across the organisation, allowing every employee to have access to the appropriate information.

SELECTING A SYSTEM OF ENGAGEMENT

For FIs, the journey to the intelligent enterprise begins with defining the desired value to be achieved through the implementation of AI and related technologies. Too many FIs begin by creating the infrastructure without first understanding the true ROI of the endeavour, instead of starting by choosing one use case that will deliver value to the organisation — whether it is streamlining the financial statement data capture in commercial lending, employing 'next product to sell' capabilities in retail customer onboarding or implementing risk-based pricing to help meet consumer fair lending compliance requirements.

FIs must then decide whether to buy or build the technology. For those organisations that do not have the benefit of massive resources to create their own software, partnering with a FinTech vendor that has the expertise, experience and a track record of success working with AI-driven data insights will likely be the better option. Regardless of approach, putting AI in place can enable FIs to increase revenue, gain operational efficiencies and better meet customer expectations. With cognitive technologies, FIs can offer employees the opportunity to do more for their customers, while saving valuable time.

CONCLUSION

For FIs, the idea of undertaking a digital transformation and abandoning old, comfortable ways of doing business can be daunting. Nonetheless, the COVID-19 crisis, with its broad business shutdowns and stay-at-home orders, proved that cloud-based, digital capabilities have become an important component of a sustainable business model for most FIs. Even as countries around the globe gradually reopen, the financial services industry, and indeed the world itself, will remain forever changed.

In a post-pandemic world, FIs have an opportunity to revolutionise their market offerings in terms of speed-to-market and flexibility using AI and the cloud. Those organisations that hesitate to implement these transformative technologies may find that they face even stronger headwinds in the future. The FIs, however, that are able to effectively execute on a digital strategy through the right talent, focus and adoption of the cloud and cognitive technologies will be the winners in the long term and prosper in this new age of banking.

References and Notes

1. Bellens, J., and Meekings, K. (February 2020) 'Why global banking profitability will remain a challenge in 2020', *EY*, available at: https://www.ey.com/en_gl/banking-new-decade/why-global-banking-profitability-will-remain-a-challenge-in-2020 (accessed 2nd March, 2021).
2. Digital Processing. (October 2018) 'Google Cloud helps BBVA work in a more agile and collaborative way', *BBVA*, available at: https://www.bbva.com/en/google-cloud-helps-bbva-work-in-a-more-agile-and-collaborative-way/ (accessed 2nd March, 2021).
3. Santander Technology. (April 2019) 'Technology, talent and size to underpin Santander's strategy', available at: https://www.santander.com/en/stories/technology-talent-and-size-to-underpin-santanders-strategy (accessed 2nd March, 2021).
4. Celent Case Study: Santander UK. (April 2020) 'Santander UK wins Celent model bank award for commercial lending in partnership with nCino', *nCino*, available at: https://www2.ncino.com/news/case-studies/celent-case-study-santander-uk. (accessed April, 2021).
5. Hypervisor is computer software, firmware or hardware that creates and runs virtual machines.
6. Cloud Act. (2017–2018) 'Clarifying lawful overseas use of data act', available at: https://www.congress.gov/bill/115th-congress/house-bill/4943. (accessed April, 2021).
7. GDPR: General Data Protection Regulation. (n.d.) 'Regulation specific to privacy and protection of data in the EU. It also applies to transfer of personal data outside the EU', available at: https://www.trendmicro.com/vinfo/in/security/definition/eu-general-data-protection-regulation-gdpr. (accessed April, 2021).
8. Salesforce, Customer 360 Platform. (n.d.) 'Silver linings: Why your data is safer in the cloud', available at: https://www.salesforce.com/products/platform/best-practices/improving-cloud-security/. (accessed April, 2021).
9. Salesforce. (n.d.) Further information about Salesforce and security can be found at: https://trust.salesforce.com/en/. (accessed April, 2021).

10. Amazon. (n.d.) 'Shared responsibility model', available at: https://aws.amazon.com/compliance/shared-responsibility-model/. (accessed April, 2021).
11. *Ibid.*, ref. [9] above.
12. Host regulator: the country where the firm has its HQ acts as the host regulator, and authorisations are obtained through this route. These can be 'passported' to other jurisdictions.
13. EBA. (October 2019) 'Final report on EBA guidelines on outsourcing arrangements', further guidelines have been issued by other authorities, available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf. (accessed April, 2021).
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 organisation 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 commission. (n.d.) 'European cloud strategy 2012', available at: https://ec.europa.eu/digital-single-market/en/european-cloud-strategy-2012 (accessed April, 2021).
18. European Banking Federation. (n.d.) 'Cloud adoption by European banks', available at: https://www.ebf.eu/priorities/innovation-cybersecurity/cloudbanking/.
19. EU Cloud Code of Conduct. (n.d.) 'Your path to trusted cloud services in Europe', available at: https://www.ebf.eu/priorities/innovation-cybersecurity/cloudbanking/.
20. EBF Press Release. (n.d.) 'Two years on: EBF cloud banking forum', available at: https://www.ebf.eu/innovation-cybersecurity/twoyearscloudbankingforum/.
21. World Economic Forum. (February 2020) 'Transforming paradigms: A global AI in financial services survey', available at: https://www.weforum.org/reports/transforming-paradigms-a-global-ai-in-financial-services-survey.
22. Accenture. (4 April 2018) 'Realizing the full value of AI in banking', available at: https://www.accenture.com/_acnmedia/PDF-77/Accenture-Workforce-Banking-Survey-Report (accessed April, 2021).