



THE COMING OF CLOUD

CLOUD COMPUTING AND WHAT IT MEANS
IN THE PAYMENTS SPACE

CLOUD COMPUTING AND WHAT IT MEANS IN THE PAYMENTS SPACE

- By 2018, approximately two thirds of global financial services will be using cloud computing for significant infrastructure needs.
- By 2019, top tier banks will be able to reduce their capital expenditure on infrastructure by 25 per cent thanks to cloud adoption.
- Cloud will become the 'fundamental technology' that underpins the digital transformation of banking¹

These are bold statements for an industry that has traditionally been resistant to the allure of cloud

technologies. Nonetheless the confidence of IDC analysts is shared by researchers at Deutsche Bank, who have predicted that cloud technologies would account for 20-30 per cent of some banks' operations by 2019.

A sense of confidence has emerged around cloud in financial services, particularly in payments. The widely-held idea among commentators and analysts is that 2017 is the year that cloud will take off in financial services. In this paper, we take a look at why cloud has accelerated up the agenda – and what banks should be doing next.

TABLE OF CONTENTS

1 [BANKING AND THE CLOUD: WHERE ARE WE NOW?](#)

2 [RECOGNIZING THE BENEFITS: A SOPHISTICATED OFFER](#)

3 [DRIVERS FOR CHANGE 1: A SHIFTING LANDSCAPE](#)

4 [DRIVERS FOR CHANGE 2: REGULATORY SUPPORT](#)

5 [DRIVERS FOR CHANGE 3: RESPONSIVE PROVIDERS](#)

6 [ADOPTING CLOUD](#)

7 [CONCLUSION](#)

1. BANKING AND THE CLOUD: WHERE ARE WE NOW?



This change of atmosphere is a distinct move from the general belief within the industry that it would take several more years for payments to embrace the cloud. The conversations about cloud in financial services have grown more intense over the past two years, but critical areas such as payments have often fallen outside the discussion.

As BBVA noted in 2016², banks were already widely using cloud computing for non-core and non-critical uses, such as human resources, e-mail, customer analytics, customer relationship management, and development and testing. By June 2015, 87.5 per cent of financial services firms in the EU had used cloud services at least once³ - much of it focused on these commodity functions. Consider that standard office packages from Microsoft, Google Docs, and other basic software tools run on the cloud, this is perhaps not surprising.

However, that's not the complete picture. BBVA went on to cite a number of smaller banks that have either transferred entire core services to the cloud, or are in the process of doing so. Independence Bancshares in the US, Zitouna Bank in Tunisia, My Community Bank in the UK, and ME Bank in Australia are given as examples of smaller players that are delivering treasury, payments, retail banking, or enterprise data via the cloud.

Elsewhere, banks may be further along the path to cloud than many vendors believe: 80 per cent of banks in Asia Pacific, for example, are expected to run on a hybrid cloud architecture by 2018 according to IDC. Of course, there

are a number of major players that have wholeheartedly embraced cloud technologies for mission-critical systems.

In November 2016, Capital One became one of the highest-profile names to fully embrace the public cloud. Over the next five years, Capital One will continue to migrate many of its core business and customer applications to Amazon Web Services, as part of its digital strategy. The company is also closing data centers in favor of cloud-based storage. According to Rob Alexander, Capital One's CIO "There's nothing we aren't willing to put in the public cloud."

Spotlight on DBS Bank

Singapore's DBS Bank has signed an agreement with Amazon Web Services to take advantage of its cloud technology. DBS plans to create a hybrid cloud environment that is optimized for rapid changes in capacity as well as functionality. The hybrid cloud will provide a complementary service to the banks' traditional data centers.

2. RECOGNIZING THE BENEFITS: A SOPHISTICATED OFFER

So what accounts for the new-found confidence and the acceleration of cloud adoption? Partly it's greater recognition of the benefits on offer. The traditional argument – that cloud delivers cost savings and enables firms to focus on what they know without being distracted by IT maintenance – certainly still applies. However, it's a rather simplistic view of the advantages that cloud delivers to IT teams, business users, customers and partners – depending on the 'flavor' of cloud being adopted. With early adopters benefitting from one or more of the following, others are keen to experience the same:

1. Significant reduction in capital and operational expenditure across the IT estate as responsibility for purchasing sufficient computational power plus ongoing maintenance and upgrades falls to the cloud service provider – who offer economies of scale.
2. The ability to redeploy internal IT experts towards more productive or value-add activities, such as strategic operations, or one-off pilots and proofs of concepts.
3. Improved security of data in transit as banks take advantage of in-depth expertise embedded in cloud service providers' operations, in addition to their ongoing investment in the latest security measures and techniques, fail-over, resilience, and business continuity.
4. Greater responsiveness and agility in business operations as processing power can be spun up to provide development and testing environments, or on-demand peak performance, and spun down when no longer required, helping to align operating costs with the needs of the business.
5. Faster go-to-market for updates to existing products and services, as well as brand new innovative services that are developed on a streamlined, standardized, and open platform that no longer hindered by internal bottlenecks, choke-points, or duplications.
6. Elimination of prohibitively long lead times caused by insufficient processing power, or the costs and bureaucracy required to scale up their hardware, infrastructure, and support capabilities.
7. A greater risk tolerance thanks to an ability to enter and exit new markets without significant investment in new infrastructure.
8. The ability to experiment with and explore the benefits of new technologies, such as blockchain, containers, micro-services, server-less computing, software-defined WAN (SD-WAN), and the Internet of Things (IoT), in a cloud environment without diverting essential processor capacity away from core services.



3. DRIVERS FOR CHANGE 1: A SHIFTING LANDSCAPE

As the benefits of cloud deployments begin to crystallize, their relevance has become more acute. Siloed systems often lack the scalability, flexibility, and reliability needed to meet the following demands. As IT provision is reviewed more generally, cloud inevitably becomes part of the conversation.

1. Banks are under pressure to upgrade applications to respond to growing customer needs. The change in expectations from consumers and SMEs when it comes to payments is gathering pace. Demands for real-time, personalized, and seamless services across all channels and all devices, are driven in part by familiarity with the 'one-stop' digital services offered by firms like Uber, which bring functions like finding a route, booking a car, and arranging payment in a single user-friendly app.

As a result, issuers and acquirers globally are continuing to invest in their payment capabilities. However, as we note in our paper on high availability, in many cases current infrastructure, with its siloed data and stovepiped functions has been pushed to its limits. Modernization strategies are required to meet the demands of omni-channel, needs-centric banking, and payments.

2. That demand from customers is accompanied by a rapidly changing environment in which most financial institutions operate. The FinTech ecosystem is flourishing, with successful niche players founded on business models that are typically more responsive to internal and external forces, and have both a finger on the pulse of customer demand and a higher risk tolerance.

In the face of the innovations delivered by these disruptive, digital-first players, traditional financial institutions need to go beyond traditional means of engagement: investment or acquisition. They can either co-opt the technologies through partnership or face disintermediation from one or more areas of business. For those that choose to stay competitive or engage productively in relationships with FinTech

companies, new ways of thinking need the support of new ways of managing data and infrastructure.

3. Thirdly, there is the move towards Open Banking. The new relationships with FinTechs are in part inspired by the sharing ethos of Silicon Valley and the growth of the 'hackathon' in other successful business areas. Once seen as extremely risky in the heavily regulated world of big banks, hackathons are now used by those hoping to harness innovation and with it the mercurial millennial customers.

Consequently, some of the world's largest financial institutions, including Santander, Barclays, Citibank, BNY Mellon, First National Bank, and Royal Bank of Canada continue to host hackathons in the search for fresh approaches to software and fresh talent.

In addition to this more organic development, regulation is now mandating a more open approach. The goal of the EU's Revised Payment Services Directive (PSD2), for example, is to enhance consumer protection and convenience, improve the security of payment services and promote innovation and competition among all kinds of payment services by opening up access to accounts through the use of open APIs. Cloud can play an essential role here, through services such as API gateways, identity and access management as a service, or cyber security as a service.

In this changing landscape, current methods of delivering payment solutions – in terms of applications and infrastructure – are under threat. The primary goal of Open Banking and open APIs may be to change the way banks think about products and distribution, but they also require a re-think in terms of infrastructure. According to a 2015 survey from Finextra⁴ plenty of banks consider the requirements of PSD2 compliance as a catalyst for a wider payments modernization program – but only five per cent were convinced that their core-banking platform was fit for purpose in this newly open environment.

4. DRIVERS FOR CHANGE 2: REGULATORY SUPPORT

When financial services firms first started deploying cloud technologies the focus was inevitably on private cloud solutions that were owned and managed in house. Given the number of regulations to be followed in areas such as data protection, and the high consequences of security breaches, many banks felt that moving operations to public cloud tools constituted too high a risk. However more recently, there has been greater interest in public and hybrid alternatives that offer a combination of different deployment and services models.

In part this is because regulators worldwide have started to embrace cloud provision⁵ as a viable option for the companies they oversee. Research from the European Union Agency for Network and Information Security shows that when this happens, cloud adoption by financial services firms rises significantly⁶ – a trend that points to strong pent-up demand for cloud in the financial sector.

In the UK, the Financial Conduct Authority has said: “We see no fundamental reason why cloud services (including public cloud services) cannot be implemented with appropriate consideration, in a manner that complies with our rules.” Its commitment to cloud is in line with statements from other regulators in, for example, the Netherlands, Australia, Switzerland, and Japan.

Concerns about data residency are also being alleviated. A number of cloud service providers are also able to deliver their services from different national jurisdictions to ensure that customer data remains compliant with

relevant regulation. Both Microsoft and Amazon have set up services in Ireland, for example, to ensure that data remains in the EU, which currently meets the UK Information Commissioner’s Office requirement for data residency and compliance with the Data Protection Act.

The second hurdle – security – is also being overcome. It is generally recognized that cloud providers can and do hold security accreditations and certifications that are more rigorous and extensive than those held by individual financial institutions. Adopting public cloud provision ensures banks comply with:

- Industry-acknowledged standards such as ISO 27001, ISO 27017, and ISO 27018
- Demands of regulatory bodies including PCI compliance and Health Insurance Portability and Accountability Act (HIPAA) compliance.
- Government-certified schemes such as the National Institutes of Standards and Technology (NIST) in the UK and Federal Information Processing Standards (FIPS) in the US.⁷

On a more technical note, cloud providers also have the potential to dynamically re-allocate resources in order to carry out filtering, traffic shaping, encryption and other services that increase support for defensive measures. This can provide far greater protection against a distributed denial of Service (DDoS) attack through predictive and preventative action, or by protecting data during the course of an attack.



5. DRIVERS FOR CHANGE 3: RESPONSIVE PROVIDERS

None of this has gone unobserved by public cloud providers, who have been watching closely and have started to actively target financial institutions.

For example, Amazon Web Services has recently launched its Financial Services Competency Program, which aims to certify technology and consulting partners in the financial services sector. Meanwhile, rival Microsoft has developed

a new version of software on the MS Azure platform that allows it to offer cloud banking capabilities to companies that have traditionally used on-premise solutions. Of the world's 38 largest financial institutions and insurance companies, 25 have already signed up with Microsoft and are beginning to put applications in the cloud⁸.

6. ADOPTING CLOUD

In practice, more and more banks will need to adopt a 'cloud-first' or 'cloud-native' mindset, in which the cloud will be the primary consideration when evaluating changes to their IT estate. With IDC predicting that half of all banks will adopt disruptive technologies including cognitive, robotic process automation, and blockchain by 2020, and that this will accelerate digital transformation by 30 per cent, big changes are afoot. As the amount of data and demands of applications grows, it will become increasingly difficult for banks to cost-effectively manage their own data centers.

Nonetheless, it's important to recognize that when it comes to migrating services to cloud, there's no such thing as a standard solution. This in and of itself is a major challenge, and it's important to strike a note of caution here. Dealing with an ever-increasing level of complexity, thanks to the sheer number of different types of cloud services on offer, different pricing models, different business goals and diverse strategies means that migrating to cloud has to be undertaken with the same strategic, considered, and phased approach as any other aspect of IT migration.

What's more, with the cloud-computing environment becoming as complex as most traditional data centers, it now requires management and support functions to be integrated with monitoring and planning functions to ensure organizations are getting the best value from the services being used. There is a real risk that banks could

simply transfer the complexity and sclerosis of current systems to the cloud. A silo in the cloud is still a silo – and does little to overcome the challenges or take advantage of the opportunities that banks currently face.

More specifically, a number of key IT challenges need to be addressed to accelerate cloud adoption, as follows:

1. Encryption

Most card schemes or networks require a hardware security module (HSM) to undertake essential encryption tasks. This involves the use of institution-based encryption master keys from which other key types are derived. In a cloud environment, each application would need reasonably local access to several HSMs and its master keys.

However, a round trip to an HSM is one of the most expensive tasks in transaction processing. A single transaction may require as many as five such trips just to check message authentication and PIN-block translation. Because each of these steps are performed at a different stage of the processing cycle, the HSM needs to be as responsive as possible.

Cloud-ready HSM solutions are still rare – and anecdotal evidence suggests that, in the field, those that are available may not yet be as responsive as needed.

2. Multi-tenancy

One of the main assumptions of a true cloud solution is that it operates in a multi-tenant environment in which a single instance of the software serves several users or groups of users (the tenants) from a single server or server cluster.

For most applications, this is reasonably straightforward: users log in to the application to access only the data relating to their own organization. This in turn requires a reasonably simple implementation with a discerning column in the relevant database tables identifying which organization owns what data.

However, for payment and transaction processing on solutions like NCR's Authentic, the multi-tenant environment creates its own challenges. Today, Authentic provides a high level of multi-organizational support at both the device and the issuer data level. However, in a multi-tenancy environment, an individual tenant may be processing on behalf of multiple organizations. This extra layer of complexity must be addressed in order to effectively manage application access, data and security for hundreds of users.

3. Data consistency

In distributed environments where an application is available in multiple locations, data needs to be quickly,

easily, and consistently replicated between sites.

This ensures that every user has access to the latest information and every transaction is authorized with the most up-to-date data.

The atomicity, consistency, isolation, and durability (ACID) properties of a relational database management system (RDBMS) have traditionally met this demand and ensured that all updates during a transaction are captured in a consistent fashion. The ability to provide a level of assurance regarding data accuracy at all points of the transaction reduces the likelihood of a customer dispute, making RDBMS the ideal tool for this type of application.

However, RDBMS often require a third-party solution to replicate data and resolve clashes arising from data being simultaneously modified at more than one site – a sign of the challenge presented by a hyper-distributed cloud deployment. In many cases, the emergence of No-SQL databases with their in-built data replication, faster updates and better response times is the ideal solution. However, without the ACID properties or referential integrity of an RDBMS, they are yet to be proven for a payment platform – and persisting data and meta data across a massively distributed installation needs to be addressed.

7. CONCLUSION

Cloud is a transition: for banks, for their customers, partners, and vendors. As demand increases, and ability to deploy securely in private or public cloud grows, more vendors and developers will work to overcome the technology challenges, and more and more solutions will make the move to a cloud-based, utility model.

In the meantime, as banks explore their cloud options with an increasing sense of urgency, they should work both with cloud-service providers and their preferred vendors to develop both their strategic vision – and a plan for successful, stable and secure implementation.

¹IDC: MaturityScape Benchmark: Cloud in Banking in Asia/Pacific. 2017

²BBVA: Cloud banking or banking in the clouds? 29 April, 2016

³European Union Agency for Network and Information Security: Secure Use of Cloud Computing in the Finance Sector. December 7, 2015

⁴Finextra Research Ltd: *PSD2 and XS2A – Regulation or Opportunity?* 2015

⁵European Union Agency for Network and Information Security: *Secure Use of Cloud Computing in the Finance Sector*. December 7, 2015

⁶European Union Agency for Network and Information Security: *Secure Use of Cloud Computing in the Finance Sector*. December 7, 2015

⁷Amazon Web Services: AWS Cloud Compliance; Microsoft Trust Center: Compliance – Industry verified conformity with global standards; Google Cloud Platform: Google Cloud Platform Security

⁸Bloomberg: Banks Look Up to the Cloud as Computer Security Concerns Recede <https://www.bloomberg.com/news/articles/2016-07-28/banks-look-up-to-the-cloud-as-computer-security-concerns-recede>. Retrieved 18 July 2017



CONTACT US AT NCR.COM TODAY

ABOUT AUTHENTIC

Authentic is an intelligent transaction-processing platform designed for today's fast-changing payments business. It has become the payments engine of choice for issuers, acquirers, payment service providers, ISOs and merchants around the world. Part of NCR's CxBanking software suite, [Authentic](#) unlocks amazing consumer experiences across physical and digital banking channels.

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR representative or NCR office for the latest information.

NCR is a registered trademark of NCR Corporation in the United States and/or other countries. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.

© 2017 NCR Corporation Patents Pending

17FIN8094-1017

ncr.com

