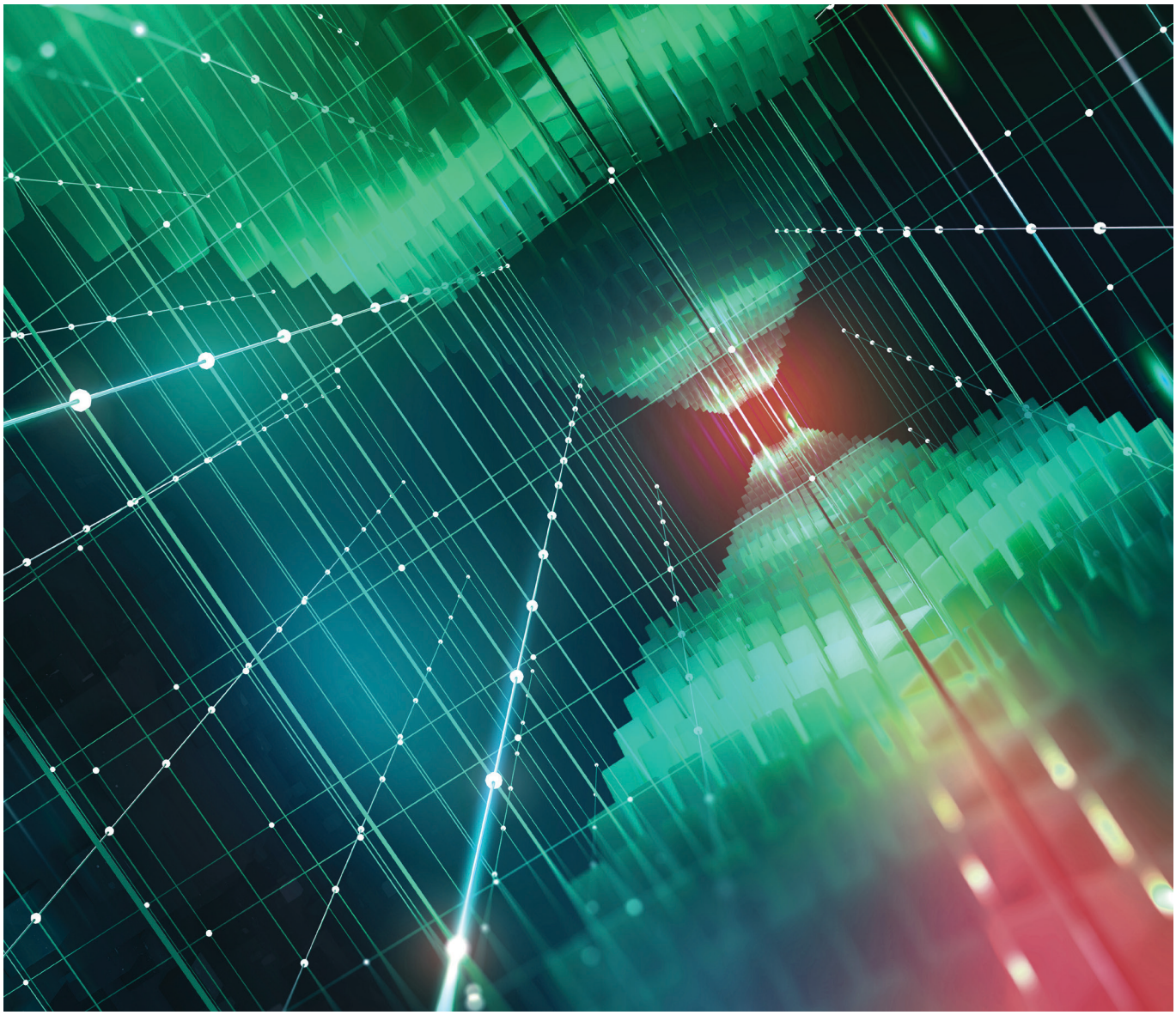
afme/
Finance for Europe

The Adoption of Public Cloud Computing in Capital Markets

November 2019



Association for Financial Markets in Europe
www.afme.eu

Disclaimer

The Adoption of Public Cloud Computing in Capital Markets (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

November 2019

Executive Summary

As an enabler of innovation and technological transformation, cloud computing is one of the key technologies that has the potential to shape the development of Europe's capital markets in the next five to ten years.

This first paper by the AFME Cloud Computing Task Force sets out a number of recommendations for banks, cloud providers and regulators to help realise the full potential of public cloud computing across the industry.

Cloud is a versatile technology which can be used in a variety of ways, providing infrastructure, platforms and software to users. It can be set up for exclusive use by a single organisation, or as an open resource for multiple organisations. The latter model, known as public cloud, is the focus of this paper, as it is a current area of growth which is attracting interest from regulators.

Public cloud adoption within AFME's members is driven by a number of key benefits. These include greater business agility and innovation; improved overall cost management; increased operational efficiency; enhanced client experience and service offerings; and effective risk mitigation.

There is a range of use cases where public cloud is currently being applied. For example, where a burst of computing capacity is required (such as supporting trade processing at peak hours of demand) to applications that need to be quickly configured and delivered across business units (such as client relationship management systems). While deployment is currently focused on non-material processes, there is an increasing willingness to explore migration of other systems to the public cloud.

However, the ability of the capital markets industry to adopt public cloud at scale will be dependent on the extent to which current barriers can be addressed. Some of these barriers are internal to firms, for example the challenges of legacy IT architecture, but some are industry wide, spanning regulatory uncertainty and constraints, as well as a lack of technical awareness regarding the benefits and risks of public cloud. In response, banks are developing and refining their public cloud strategies, transforming their existing ways of operating and creating new models for working with cloud providers.

This paper puts forward 14 recommendations in support of continued public cloud adoption. The recommendations – subdivided against banks, cloud providers, regulators, and the industry as a whole – aim to increase the transparency and collaboration required to build further confidence, trust and capability in public cloud.

AFME and its members look forward to discussing the recommendations with all industry participants and continuing to support public cloud adoption in capital markets.

1. Introduction

In our September 2018 report, 'Technology and Innovation in Europe's Capital Markets', AFME members identified cloud computing as one of four key technologies with the potential to transform investment banks ('banks') and the industry. In particular, cloud computing was identified as a foundational requirement for enabling most other new technologies and innovations, and for driving future IT and business change.

However, the survey also found that only 29% of respondents believed there would be strong adoption of public cloud across the industry in the next five years. Several constraints on the widespread adoption of public cloud included areas such as legacy IT complexity, perceptions about cross border information security, and legal and regulatory concerns.

Today, banks are more actively exploring and adopting new technologies, such as public cloud, to drive innovation, increase security, provide better services for customers and maintain their competitive position in the face of new market entrants. At the same time, the use of public cloud remains an important topic for banks, policymakers and regulators, in seeking to ensure that its wider adoption does not pose unforeseen risks to the secure, reliable and efficient operation of financial markets, and the safe handling of client transactions and data.

This paper has been developed, with expertise from AFME Member firms, and Premium Associate Members, to provide further assessment of public cloud adoption in capital markets as identified in our 2018 report. The paper examines in more detail:

- The drivers and benefits for public cloud adoption;
- Where and how it is being adopted today;
- Barriers to change; and
- How adoption is being progressed within banks.

The paper concludes by providing a set of recommendations for banks, cloud providers, regulators and the industry as a whole, for supporting the continued adoption of public cloud in capital markets.

2. Cloud Computing and its Benefits

This section provides context on cloud computing and examines the reasons behind the increasing importance of public cloud to financial services.

Cloud Computing

Cloud computing offers an adaptable and versatile way to consume a range of information technology (IT) services, such as business applications, data storage or processing power. Cloud is offered 'as a service', where IT resources are provided on-demand and the location of the physical hardware, application or data is largely extraneous to the users.

Cloud computing is rapidly becoming the norm for IT processing and data storage solutions offered both by major and niche vendors[1]. Technology upgrade and refresh is a routine requirement for most banks, and cloud computing options are attracting increasing interest from business users and Chief Information Officers (CIOs) looking to enhance their capabilities and increase efficiency.

There are three high-level service types for cloud computing: the provision of underlying IT infrastructure such as servers (Infrastructure as a Service - IaaS), platforms such as databases or operating systems (Platform-as-a-Service - PaaS), and end-user software and applications (Software-as-a-Service - SaaS). In each service type the data remains in the ownership of the client. Further detail on each of these three services is provided in Table 1 below.

Table 1: Cloud Computing Services[2]

Cloud services	Description of services	Example
IaaS (Infrastructure-as-a-Service)	Consumers can provision fundamental computing resources where they are able to deploy and run arbitrary software. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components.	Grid or High-Performance Computing (HPC)
PaaS (Platform-as-a-Service)	Consumers can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting. environment.	SQL database, Database Platform-as-a-service (DPaaS)
SaaS (Software-as-a-Service)	Consumers can use the cloud provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.	Customer Relationship Management (CRM) application

These three cloud computing services can be hosted in a range of different models (either by selecting one or by using a multi-cloud strategy). These are:

- **Private Cloud:** The cloud infrastructure is provisioned for exclusive use by a single organisation. It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises;
- **Community Cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises;

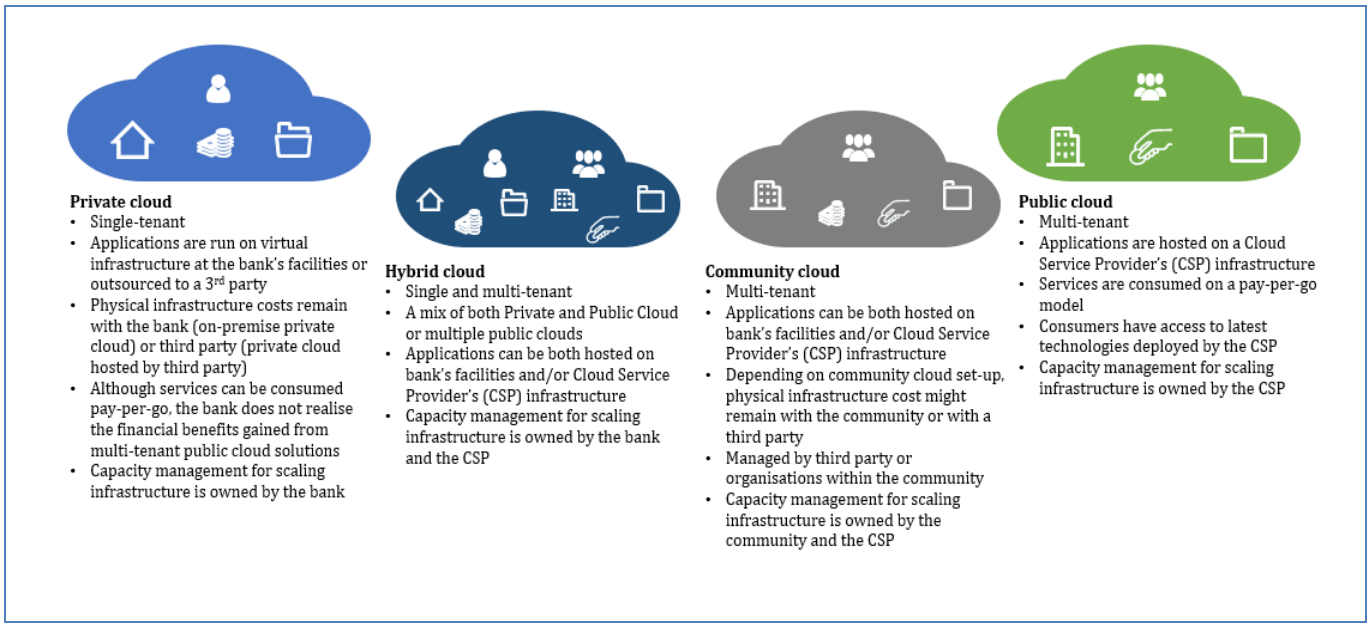
[1] For example, a survey by Synergy Research Group in 2019 across seven key cloud service and infrastructure market segments, shows that operator and vendor revenues for the first half of 2019 passed the $150 billion milestone, having grown by 24% from the first half of 2018. In the cloud service segments, IaaS & PaaS had the highest growth rate at 44%, followed by enterprise SaaS at 27%. See https://www.srgresearch.com/articles/half-yearly-review-shows-150-billion-spent-cloud-services-and-infrastructure

[2] Source – National Institute of Standards and Technology (NIST)

- **Public Cloud:** The cloud infrastructure is provisioned for open use by multiple organisations. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider; and
- **Hybrid Cloud:** A composition of public and private cloud that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability.[3]

Further detail on each of these four cloud computing models is illustrated in Figure 1 below.

Figure 1: Four models of cloud computing[4]



Our members identified that their current preferred model for cloud adoption within financial service is a hybrid model which can deliver benefits from adopting both public and private cloud services. Increasingly, firms are starting to apply a more strategic 'cloud first' approach where all new projects and changes to existing technology and processes are considered in the cloud before any other means.

Public Cloud and the Benefits for Financial Services

For this paper we have chosen to focus on public cloud, whether as part of a hybrid model or as standalone. Spend on public cloud across all industry sectors is expected to reach $331bn in 2022, compared to $210bn in 2019[5]. Of this, financial services now account for 10.6 percent of this total, as the adoption of public cloud services becomes increasingly important.

Whilst all cloud models and services are important for financial services firms, the use of public cloud is of greater interest and scrutiny within the industry today. This is largely because of the increasing adoption of public cloud within the industry (both by financial services firms and their third-party providers), and the differentiators associated with public cloud versus other models (private cloud or traditional on-premises IT).

Public cloud has different implications for the responsibilities of firms, and cloud providers, for areas such as: management of data centres and infrastructure (e.g. servers), security (e.g. data access), and risk and compliance (e.g. the applicability of regulatory requirements). Known as the 'Shared Responsibilities' model, both the bank and the cloud provider take responsibility for activities, such as security and compliance, that are required for running a public cloud service. The provider manages elements such as the provision of servers, networking and data centre facilities, whilst the bank is responsible for aspects such as customer data, security, application management and user access.

This model can also extend to sharing responsibilities for IT controls and risk management requirements (for example, both parties owning and managing a central operational risk register). Nevertheless, this shared responsibility model does not mean that banks discharge their ultimate accountability on cloud providers, as the ultimate liability for any bank activity will always be held by the bank.

[3] Source – NIST
[4] Source - PwC
[5] Source: Gartner (April 2019)

In producing this paper, we first asked our members to identify the most significant benefits driving their adoption of public cloud, which are listed below in order of importance:

- **Greater business agility and innovation,** providing computing capacity for experimentation and development (PaaS, SaaS), reducing project lead times and increasing scalability. Flexible usage allows banks to run IT workloads or applications as required, such as developing reports or data analytics, without needing to retain a large IT footprint (IaaS, PaaS, SaaS). Banks can access the latest technology (such as Artificial Intelligence and Machine Learning[6]), updates (such as instant security patches) and features (such as container technologies[7]);
- **Improved overall cost management**, as cloud adoption is generally via business-wide strategy rather than within individual business units (although adoption may start within specific functions). Consumption can be monitored at a granular level, providing greater transparency and control. Reduced spend on procuring physical hardware and facilities, such as on-premises data centres and the associated operations and maintenance required, by moving to on-demand usage of services on a pay-as-you-go basis (e.g. IaaS, PaaS and SaaS) frees up resources for upgrades to infrastructure and digital capabilities, which ultimately results in better services for clients. It should however be noted that moving workloads out of existing data centres is often complex and time intensive;
- **Increased operational efficiency**, allowing for increased speed and agility in existing IT and operations processes, through greater automation and self-service tools;
- **Enhanced client experience and service offerings**, quickly developing, testing and rolling out new products or features to bank functions and clients; and
- **Effective risk mitigation**, such as increased operational resilience to ensure continuity of service by distributing the risk of disruption across a greater range of infrastructure, both on-premises and off-premises[8].

It can be seen from the above that there are significant gains to be made from the adoption of public cloud and these are driving the trend in adoption within financial services. The next section of this paper considers where these gains are currently being realised, and how this is likely to expand over time.

[6] The European Parliament adopted in February 2019 'A comprehensive European industrial policy on artificial intelligence and robotics', which "Highlights that cloud computing has a key role to play in driving the uptake of AI; underlines that access to cloud services allows private companies, public institutions, research and academic institutions, and users to develop and use AI in an efficient and economically viable way"

[7] Container technology is the method of packaging an IT application or services so it can be run, with all dependencies, in isolation from other processes.

[8] See, for example, McKinsey, 2018, Making a Secure Transition to the Public Cloud

3. Use Cases for Public Cloud in Capital Markets

Considering the benefits identified in section two, we asked our members to highlight where public cloud is currently being adopted across banks today. From these discussions on the current usage of public cloud we understand that banks are at an early stage of adoption. Over two-thirds of members involved in our discussions estimated that only 1 - 10% of their bank's current workload was utilising some level of public cloud today.

Five key use cases of public cloud usage emerged, drawing on different benefits and service types. These are outlined in Table 2 below.

Table 2: How public cloud is being adopted today

Use Case		Service Types	Example Applications
Capacity Bursting	Supporting resource intensive processes or activities where public cloud can provide a 'burst' of computing power at scale to support existing IT.	IaaS	• Testing and development of algorithms, using large sets of historical data, as well as hypothetical scenarios • Supporting trade processing at peak times, such as around market open and close, as well as securing the ability to remain operational during unforeseen market events • Calculation of capital requirements, which may involve multiple complex simulations and calculations • In conjunction with other cloud services, such as PaaS, workloads automatically moved from on-premises applications into the cloud, e.g. end of day batch processing
Data Analytics	Providing infrastructure and tools for running sophisticated analytics on very large and complex data sets at scale, for example by harnessing Artificial Intelligence and Machine Learning tools[9].	IaaS PaaS	• Performing surveillance on trading activity to detect fraudulent transactions or market abuse • Pricing complex derivatives on a large grid of processing units • Running daily calculations of liquidity positions across large transaction datasets • Using large amounts of current and historical data for predictive analytics (using multiple inputs, such as interest rates)
Innovation	Allowing for the rapid provision of IT environments, and tools, to quickly run and assess innovation projects across the business.	IaaS PaaS	• Creating a project environment for testing new applications • Establishing new collaboration models between the project teams by working on shared cloud environments • Replacing repetitive human tasks that are source of errors by the usage of cloud Application Programming Interfaces (APIs) • Reducing the time to implement new digital-native products or services (such as product personalisation)
Third-Party Software	Providing applications that can be quickly configured and deployed across business units and to end users.	SaaS	• Customer Relationship Management (CRM) or workflow products • Connecting easily with real-time market data where the connectivity hardware and software are also provided as a service
Resilience	Providing flexibility, scale and the ability to utilise infrastructure in multiple locations in the event of a localised disruption.	IaaS PaaS SaaS	• Using cloud to improve local IT infrastructure (e.g. single site) resiliency • Replicating continuously software programs, data and logs across multiple locations • Keeping back-up copies and archives on a low-cost storage facility for possible future use • Leveraging multiple availability zones, regions and geographies to ensure operational continuity during a disruption

[9]For more information, see AFME's white paper 'Artificial Intelligence: Adoption in Wholesale Capital Markets', available at https://www.afme.eu/globalassets/downloads/briefing-notes/2017/afme-tao-ai-adoption-in-capital-markets-18-apr-2018.pdf

The five uses cases above are largely being used to support non-material processes or those which do not require the exchange of sensitive data. Increasingly however, financial firms are indicating readiness to migrate material processes, as well as material systems (such as those that manage transactions or end of day batch processing).

Public cloud is therefore expected to expand significantly across all areas of the capital markets value chain. Nonetheless, there are at present several barriers to this adoption within capital markets, outlined in section four, which are limiting this potential transformation.

4. Barriers to Change

Any organisation undertaking significant technology transformation will face barriers to change. In the same way, the ability of banks to adopt public cloud and achieve the benefits identified in section two will be dependent on the industry's ability to address such barriers. This is especially important given the role of cloud as an enabler of other technologies and new ways of working.

This section provides examples of some of the most significant barriers associated with banks adoption of public cloud. Whilst neither exhaustive nor exclusive to public cloud (many of the barriers may apply to any large-scale technology change), they serve to illustrate the key challenges for adoption today.

<u>The adoption of public cloud at scale is challenging for established banks, due to legacy IT architecture, the need for significant long-term commitment and conflict with existing priorities</u>

- The business-wide cloud strategies of most banks are at a relatively early stage, with the adoption of public cloud still largely taking place in specific functions and activities of the bank (as highlighted in section three). Adoption at scale will require more significant change to banks IT architecture and existing operating models. For example, ongoing costs will need to be managed on a consumption ("pay-per-use") basis, rather than a fixed-cost basis for owned infrastructure; the latter needing to be substantially downsized to achieve overall cost reduction or cost neutrality.
- The transition to public cloud beyond specific functions (such as IT test environments) to more end-to-end activities (such as trade execution and settlement) will require adjustments to embed cloud support capabilities and services and greater coordination from trading through to post-trade, risk, legal finance and compliance functions. This requires greater strategic change and investment, which may conflict with existing priorities or challenges (such as the cost of maintaining legacy technology platforms, or requiring change to established and embedded processes that address existing regulatory requirements).
- The structure and complexity of legacy IT architecture of the bank may be a barrier to public cloud adoption. Interconnected systems with complex dependencies may make the transition of specific processes or business areas to the cloud more difficult (however, after transition to public cloud, the ability to simplify and automate end-to-end activities is often easier to achieve).
- As services or functions are moved to public cloud platforms, traditional IT functions and roles (for example, database administration, networking or storage management), may not be required to the same extent. Therefore, banks often need to invest in significant training, certification and hiring to develop their workforce to support increased cloud adoption and may also need to bring in external resource in the shorter term. This current skills gap, whilst a challenge for banks, is seen equally as an issue for the industry as a whole (including regulators, financial intermediaries, existing third-party platform providers).
- Finally, there may be a shortage of, or limitation on, the availability of subject matter experts (SMEs) within the business or operations who have sufficient understanding to define and realise the target operating model to support public cloud adoption. For example, a public cloud program will require increasing levels of internal SME from dependent functions such as legal, operations, finance, risk, compliance, business continuity and HR. This is then further compounded by the need to increase the knowledge level of senior decision makers to support the SMEs in adopting cloud.

<u>Variations in the understanding of public cloud, and the risks and security implications for the industry, has led to uncertainty on its suitability and has acted as a limit on its current use</u>

- The rapid increase in the focus and adoption of public cloud has led to varying levels of maturity and understanding of the technology developing across the industry (for both banks and authorities). Concerns about the suitability of public cloud can lead to slower adoption (for example the increased reliance on third party providers, or the need for additional cybersecurity assurance compared to on-premises solutions).
- Despite widespread evidence that use of public can, when implemented correctly, bring security benefits, there remain divergent levels of understanding as to the levels, and suitability of, security and data protection offered by public cloud versus banks' existing on-premise infrastructure. For example, the European Commission has noted that, contrary to the belief that using public cloud resources would reduce its own security posture, "reality has proven that a correct usage of public cloud resources can actually increase the overall security resilience by removing internal risks"[10]. The Bank of England has also

[10] European Commission's 2019 Cloud Strategy.

recognised the potential cyber and operational benefits cloud-based models can bring, noting that by reducing time to market and increasing agility, cloud models may also offer the potential to create a more diverse financial system[11]. AFME believes that from a vulnerability perspective, the adoption of cloud can also provide an enhanced ability to identify and remediate system vulnerabilities, based on the automation and uniformity of the environment. The adoption of encryption and key management also prevents against unauthorised access data stored on the cloud.

- Additionally, new legislation, such as the 2018 US CLOUD Act[12], can lead to confusion and misconceptions on the use of public cloud (in this case the rights of access to public cloud data for government agencies; and that the Act is not just applicable to cloud providers, but also to US data and communications companies more broadly). The knowledge gap within banks, also faced by regulators and supervisors, is leading to fairly conservative approaches being taken and variations between jurisdictions on the level of public cloud understanding.

<u>A high level of recent regulatory focus on public cloud and outsourcing has created a significant level of information that banks need to absorb, and address, before greater adoption can be progressed</u>

- There has been a significant level of policy and regulatory focus on the use of public cloud over the last three years. For example, the European Supervisory Authorities (ESAs) have each issued, or plan to issue, consultations or guidelines that cover the use of public cloud. National Competent Authorities (NCAs), such as the FCA[13] (UK) and BaFin[14] (Germany), have also issued significant guidance related to public cloud over the last few years. The lack of a coordinated approach, as well as the constantly changing regulatory landscape, has had a limiting effect on the use of public cloud in the industry, particularly for medium-sized organisations with more constrained IT, regulatory resources and budgets.
- NCAs are also now focused on implementing the recent 2019 European Banking Authority (EBA) Guidelines on Outsourcing Arrangements[15] which have significant requirements that are related to the use of public cloud (for example, banks are focused on requirements such as access and audit rights; requirements on sub-outsourcing; operational resilience and exit strategies; and governance and risk assessments). Although the Guidelines have helped to harmonize the applicable regulatory framework, differences remain between NCAs' interpretations of some of the requirements, leading to the fragmented application of some criteria (such as the consideration of the prior notification requirement as an authorisation process). Depending on their implementation by NCAs, the new Guidelines could lead to a further challenge for banks if variations emerge at this level in how the requirements are interpreted. Equally, cloud providers will need to continue to familiarise themselves with the complex and changing regulatory environment of financial services and adopt compliance programmes accordingly.
- Finally, in many jurisdictions, a bank's cloud risk management framework is often more scrutinised that the product risk management framework, giving the bank more discretion in managing the product risk (which has several aspects of risks such as AML, financial, reputational etc) rather than cloud risks (which is technology, cyber & vendor risk).

<u>Variations in existing regulatory requirements - such as data localisation - increases the complexity for banks using public cloud</u>

- Different jurisdictional requirements for the localisation of data can prevent certain activities or limit the storage of data when using public cloud, for example the 2011 German Data Protection Authority (DPA) mandatory guidelines for cloud computing contracts and additional 'Safe Harbour' compliance requirements when using a US based provider.
- EU regulations, such as the General Data Protection Regulation (GDPR), the Free Flow of Non-Personal Data Regulation (FFND)[16] and the 2019 EBA Guidelines on Outsourcing, have made significant progress in clarifying, or removing, regulatory inconsistency such as data localisation requirements. However, variations remain at the Member State level, especially in data location requirements, and continue to add complexity for the adoption of public cloud at scale for cross-border banks and limit the security and

[11] Bank of England, 2019, 'New Economy, New Finance, New Bank'
[12] https://www.congress.gov/bill/115th-congress/house-bill/4943. See also the US Department of Justice white paper from April 2019, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act"
[13] https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
[14] https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.pdf?__blob=publicationFile&v=4
[15] https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements
[16] Regulations (EU) 2016/679 and 2018/1807

resilience posture of the industry.

There are no standard requirements for maintaining a register of outsourcing arrangements, including public cloud outsourcing, which banks can use consistently for reporting to authorities

- The 2019 EBA Guidelines on Outsourcing require that banks should maintain an updated register of information on all qualifying outsourcing arrangements (including public cloud) as part of their risk management framework. However, there is currently no standard industry or cloud provider approach[17], and regional and national authorities may require different levels of information over time.
- This variation could be a challenge if banks are unable to meet specific requests (for example, if a bank must clearly show a separate contract for IaaS or PaaS services provided by a single provider), or if significant ongoing maintenance of the register is required (for example, if updates are required for changes to the storage of data in a given region, or if the tactical use of temporary cloud environments for testing or development activity need to be recorded).

There is a lack of standardisation in cloud provider services, both contractual and technical

- As with many forms of outsourcing, cloud providers have varying terms of service, for example how routine maintenance (such as patching) is performed and the obligation for providing prior notification. Whilst the majority of cloud providers offer terms of service which can address specific regulatory requirements (for example, having a financial services addendum), and can work with banks to negotiate bespoke requirements (for example, accommodating different banks' compliance requirements)[18], it is a challenge to a fundamental principle of the cloud provider model, which is 'one-to-many' rather than 'one-to-one' (such as traditional outsourcing). This makes contractual negotiation burdensome as not all cloud providers are able to meet banks' requirements, and contractual differences between providers increase the complexity for banks wishing to use multiple cloud services or adopting a hybrid model with multiple providers.
- From a technical perspective, these differences are amplified, since the lack of standardisation, portability and interoperability across different cloud provider offerings may result in banks refraining from moving to the cloud, as they perceive that this could be challenging for their longer-term strategy or present a risk to their client services. In particular, they may be concerned about being 'locked-in' to contracts or services, hampering their flexibility and agility and increasing their costs.

Concentration risk in relation to cloud must be a consideration for long-term adoption and strategy

- The concentration of data, and critical financial activities, within a limited number of cloud providers could increase financial or market risk at the industry level in the event of systemic issues (for example, one or more providers becoming unavailable for a period of time).
- An increasing number of third and fourth parties are also adopting public cloud services to host their services, which will further increase potential indirect concentration risk to banks. For example, a SaaS provider may use a global cloud provider either directly to host their application, or indirectly for storing data backups or recording log files. Similarly, market data providers are increasingly beginning to use cloud technology, with data delivered onto the cloud and connectivity to the data feed embedded as a service.
- Banks, and organisations from other industries, prefer to use the hyperscale[19] cloud providers as they have greater capacity to address regulatory requirements in different jurisdictions and provide higher levels of resilience and security capabilities. However, this further increases the potential concentration risk that would manifest between the banks, the impacted provider, and other industry participants who may also be using the provider.

[17] We note that the European Banking Federation (EBF) is currently developing a cloud register to support the financial services industry.
[18] The 2019 EBA Guidelines on Outsourcing requires that banks should at least be able carry out a risk assessment of a proposed material sub-outsourcing change before coming into effect.
[19] The use of cloud computing, and providers, that can scale significantly large compute resources (servers) and environments (location of compute)

Further considerations on concentration risk

Banks can mitigate potential concentration risk by adopting a multi-provider approach (for example, using two or more regional or global cloud providers for substitutability or distributing workloads). Banks can also adopt hybrid cloud models that may also use a range of providers (for example, retaining on-premise and/or private cloud capabilities for critical activities or for business continuity purposes). These models therefore mitigate risks associated with individual cloud environments; greater focus from cloud providers on portability and interoperability between services will be key.

Whilst these actions may help to manage a bank's own concentration risk, they do not address the risk at the industry level. There are currently several parallel discussions on this topic taking place with varying authorities at the regional and global level. These discussions are considering both why there is a potential need for future regulation of cloud services and providers (for example, to address cyber and/or systemic market risks), and how this could be implemented (for example, sector-agnostic or financial markets specific)[20].

It will be important that any approaches pursued are properly assessed and do not conflict in such a way as to place additional complexity or potential restrictions on cloud adoption. Nonetheless, encouraging increased competition within this market should be a priority over the longer term.

[20] See, for example, the Institute of International Finance paper, 2019, 'Cloud Computing in the Financial Sector Part 3: Cloud Service Providers'

5. How Public Cloud is Being Progressed Within Banks

The barriers identified in section four highlighted some of the challenges for public cloud adoption in capital markets. However, banks and cloud providers are applying a range of initiatives to address some of these barriers. Four example initiatives are outlined below and are intended to inform the wider industry on what actions are already being taken, and to share lessons learned, as public cloud adoption continues to increase.

Executing a long-term public cloud strategy

- A longer-term (3–5 year) strategy and roadmap for public cloud adoption is essential for ensuring all aspects for the change are considered across the bank (from the underlying technology or software, through to the operating model required, as well as people and skills). For example, identifying which services, applications or workloads are candidates for public cloud and the appropriate risk assessments to validate their suitability.
- A clear strategy and roadmap can also help to determine the appropriate governance model and stakeholder engagement that is required. For example, some banks have set up cloud governance committees to oversee the adoption of cloud, which includes representatives from all impacted functions (such as legal, risk, compliance, finance and technology).

Adopting new ways of working, and organisational change to benefit from public cloud

- Banks are adopting new delivery approaches and ways of working, such as DevOps[21], which is an increasingly common way that both developer and operations teams today build, test and deploy applications at greater speed and with quality and control.
- These new ways of working reflect the increased automation, as well as the speed of development and operations, which public cloud provides. For example, in the case of DevOps, public cloud solutions can provide existing bank IT infrastructure and applications team with increased control and 'self-servicing' functionality (such as the direct provision of servers or storage). This allows for a closer integration of existing roles and collaboration across existing IT and business functions.
- Whilst this change is not a prerequisite for public cloud adoption, there is a growing convergence between the cloud and approaches such as DevOps, where financial institutions use DevOps tools (e.g. automated deployment or automated testing), to get the benefits of the cloud. It is important that banks consider in advance how this wider process, including people and cultural change, is implemented.

Training and certifying business and IT teams across the bank in public cloud tools and services

- Many public cloud platforms have training programs and certifications that have been developed specifically to build skills and develop best practices for their users. To support the adoption of public cloud, banks (and other industry participants, such as regulators) are using these tools to upskill and inform their IT teams as well as the wider business.
- This wider roll-out of training and engagement across both IT and the business can help banks become more knowledgeable, and effective, in their adoption of public cloud and help with reskilling teams to new ways of working.

Utilising open standards and open-source software to increase standardisation between banks and public cloud

- Open source[22] software and development is increasingly common with the use of public cloud. This is because the software can be used across a bank's cloud environment and provide a standardised way of performing certain functions, irrespective of the underlying providers. A common example is Kubernetes[23], which is an open-source software that can be used to manage IT services across an infrastructure (for example, managing network traffic or computing power across various applications).

[21] https://www.ibm.com/cloud/devops

22 Software where the original code is freely available for use (as opposed to software which has traditionally required a license.

[23] https://kubernetes.io/: Kubernetes (commonly known simply as k8s) is an open-source container-orchestration system for automating application deployment, scaling, and management. Many cloud services offer a Kubernetes-based platform or infrastructure as a service (PaaS or IaaS) on which it can be deployed. Many cloud providers also provide their own branded Kubernetes distributions.

6. Recommendations

Whilst the approaches outlined in section five above are useful in supporting the industry at this early stage of public cloud adoption, they do not, and are unable to, address all of the barriers that exist.

Therefore, based on the findings in this paper and discussions with members, we propose the following 14 recommendations for each stakeholder group - banks, cloud providers, regulators, and the industry as a whole - to support continued public cloud adoption. Many of these recommendations can be taken as applicable beyond public cloud to private and hybrid models, and should apply to IaaS, PaaS and SaaS models.

The recommendations are intended to increase the transparency and collaboration between banks, cloud providers, and regulators, as the growth of public cloud adoption continues across the industry. This continued and greater engagement will play an important role in building further confidence, trust and capability in public cloud.

Banks

Banks must continue to build their knowledge and capabilities of public cloud to support promotion of the benefits to the industry, highlighting how adoption is being progressed in a secure and controlled manner. AFME recommends that banks:

1. Design public cloud strategies with a clear vision of a realistic targeted operating model, and regularly review and reprioritise based on developments in the industry. The strategy should ensure executive sponsorship and communication throughout the adoption lifecycle.
2. Promote a 'professional of the future' culture by providing training that is regularly updated across key functions (e.g. compliance, legal, data privacy etc.), as well as senior management, and by creating internal sandboxes on public cloud. This will promote knowledge and expertise, build trust and pave the way for public cloud to be embedded across the organisation.
3. Develop monitoring capabilities for sharing information, such as security trends and emerging threats and attacks, and contribute to existing industry forums. This will support cross industry collaboration exercises that can help standardise end-to-end public cloud adoption.

Cloud Providers

Cloud providers can support banks and regulators in developing common frameworks to drive industry adoption and to meet regulatory needs. AFME recommends that cloud providers:

4. Increase engagement with banks across all levels and functions, and with regulators, to build capability and the assurances required (e.g. legal, regulatory, privacy) for public cloud use in capital markets.
5. Provide clear and detailed processes and procedures for the security and privacy of data that can satisfy industry requirements and those of regulators.
6. Support increased standardisation, particularly regarding portability of cloud services, to minimise the risk of lock-in and reduce overall systemic risk.

Regulators

Regulators have an important role in continuing to promote harmonised, and technology-neutral and risk-based legislation, for the use of public cloud at the regional and global level. AFME recommends that regulators:

7. Develop cloud understanding and expertise, and periodically review whether considering cloud as a form of outsourcing sufficiently supports financial stability and allows firms to manage their risks effectively.
8. Support European (and greater global) harmonisation in respect of requirements for public cloud (promoting a consistent framework for authorisation, adoption, management and reporting), and continue to identify and remove forced data localisation requirements which impede the ability to apply a risk-based approach.
9. Facilitate and/or participate in multi-stakeholder technology forums that support the adoption of public cloud by banks, and 'compliant by design' solutions, and aid early identification and resolution of key regulatory issues and concerns.
10. Work to ensure supervisory practice is harmonised to reduce the complexity of fulfilling regulatory requirements for the use of cloud (for example, a common deployment reporting template, access and audit rights, and interoperability).

Industry wide

The capital markets industry must continue to collaborate, share knowledge and best practice and promote standardisation and consistency in how public cloud is adopted and controlled. AFME recommends that market participants:

11. Develop a unified or common controls catalogue against which banks can engage, and assess, cloud providers against requirements such as risk, compliance and maturity. This could be developed and maintained at a global level (such as by an international standard-setting organisation) with input from banks, regulators and cloud providers.
12. Promote an open and multi-stakeholder dialogue to discuss and assess potential approaches, and the purpose, of any future regulatory approach to cloud services and providers. This should incorporate ongoing discussions at the regional (for example, European Commission) and global level (for example, the FSB).
13. Support standardisation efforts, public-private partnerships, or Centres of Excellence (CoE), where all relevant parties can share knowledge and lessons learnt from public cloud adoption.
14. Promote best practices for the safe and secure adoption of cloud computing that includes areas such as data security, systems resilience, contingency plans and exit strategies (taking into account the size, type and activity outsourced for a proportionate and risk-based approach).

7. Conclusion

This paper has examined the current drivers, benefits, use cases, barriers and approaches for increasing the adoption of public cloud in capital markets. Whilst the capital markets industry is at an early stage of adoption, the technology and services provided are beginning to bring significant benefits to banks.

As public cloud adoption continues to increase it will be vital that all industry participants – particularly banks, cloud providers and regulators – continue to collaborate and ensure the wider benefits can be achieved for all parties, and that the knowledge, skills, security and risks are appropriately assessed and identified through this long-term transformation.

Notes

Bibliography

Bank of England, 2019, New Economy, New Finance, New Bank

European Commission, 2019, The European Commission Cloud Strategy

International Institute of Finance, 2018-9, Cloud Computing in the Financial Sector Parts 1-3

McKinsey, 2018, Making a Secure Transition to the Public Cloud

P. Mell and T. Grance, 2011, The NIST Definition of Cloud Computing

US Department of Justice, 2019, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act

Contributors to this Paper

We are grateful to our member firms and the individuals who contributed their time and thoughts in producing this report. In particular, we wish to thank our Premium Associate Members.

AFME Technology and Operations

AFME's Technology and Operations Division brings together senior technology and operations leaders to influence and respond to current pan-European market drivers and policy.

The Adoption of Public Cloud Computing in Capital Markets white paper was led by the AFME Cloud Task Force as an initiative within the broader Technology and Operations Division.

AFME Contacts

Andrew Harvey
aharvey@gfma.org
Managing Director, Technology and Operations, AFME
+44 (0)20 3828 2694

David Ostojitsch
david.ostojitsch@afme.eu
Director, Technology and Operations, AFME
+44 (0)20 3828 2761

Fiona Willis
fwillis@gfma.org
Associate Director, Technology and Operations, AFME
+44 (0)20 3828 2739

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policy makers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 788 3971

Frankfurt Office
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany
+49 (0)69 5050 60590

Press enquiries
Rebecca Hansford
Head of Media Relations
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU