UK FINANCE

CLOUD ADOPTION

November 2021

In association with: pwc Google

UK FINANCE

UK Finance is the collective voice for the banking and finance industry. Representing around 300 member firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

1. Introduction

As organisations undertake digital transformations, accelerated by the pandemic of the past year, cloud adoption is increasing. Cloud has proven itself a cost-effective vehicle for reduced time to value and increased innovation potential. It is also now seen as an enabler of greater security and resilience by default, and if well engineered the foundations of a simpler and more manageable technology estate. At the same time, there remains some scepticism around the security and resilience of cloud infrastructure in this ever more connected digital world. However, when done right (and configured correctly) the benefits of the cloud can outweigh the risks.

This paper is intended to help support the financial services regulators and supervisors in their continuous assessment of the benefits and risk considerations of adopting and regulating the cloud. The subsequent sections discuss:

- Section 1 - Cloud adoption concepts
- Section 2 - Cloud benefits and misconceptions
- Section 3 - Cloud risk management
- Conclusion - Key considerations to support adoption and oversight

The vision - The value proposition cloud brings to the financial services sector

Successful cloud adoption is based on a clear value proposition that outlines the business benefits of the cloud (the opportunity) and the potential security and resilience risks and how these are managed.

Cloud presents unprecedented opportunities for the financial sector at the intersection of economies of scale, standardisation, innovation and operational resilience. For example:

- Cloud enables firms to stream real-time market information into large-scale databases and Artificial Intelligence (AI) and Machine Learning (ML) models to quantify and cost risk.
- Cloud can help firms to combat fraud and money laundering through these AI/ML models. Combining transactional and behavioural data can help more accurately detect fraud patterns and simultaneously avoid costly false positives.
- Cloud-based technologies can be leveraged for banks' own risk-management to determine liquidity and exposure more quickly, to carry out market-to-market adjustments and for better accounting in general.
- Cloud can help financial services providers to create experiences that more closely resemble the best digital ones in other industries. Today's digitally savvy firms are using the cloud to process vast quantities of information to construct and sell financial products that differentiate themselves in a highly competitive market, where customers stand to gain the most.
- The robustness and scale of cloud infrastructure, and the high availability (HA) and service-level agreements (SLAs) of managed solutions has enabled financial institutions to cater to changing customer behaviours with minimal service disruption.

Current UK financial services cloud adoption

More than half of the UK Finance members surveyed reported their cloud adoption strategy was not adversely impacted as a result of the pandemic. In fact, nearly a third agreed cloud adoption was accelerated due to the need for remote working, strategic programmes requiring multi-year investments, and building digital products where cloud best fits the purpose. These include the development of new mobile banking apps and customer service chat-bots; processing large-scale, real-time information to better manage risk such as Anti-Money Laundering (AML); understanding customer segment behaviours; and tracking market movements to ultimately gain a competitive advantage in an increasingly fierce market.

According to PwC's 2021 Global Digital Trust Insights survey (see Figure 1), only six per cent of UK financial services firms are currently fully realising the potential security and resilience benefits of cloud adoption. A major factor in realising these benefits is the time it takes to adopt, transform and normalise to a new way of working with the cloud – across people, processes and technology.

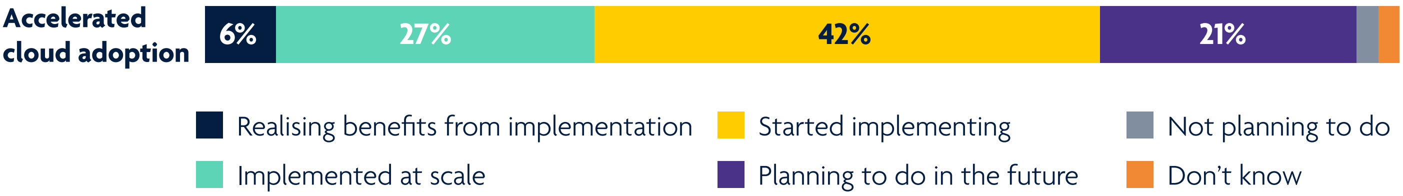


Figure 1 - PwC's 2021 Global Digital Trust Insights survey question results on cloud adoption (of 52 UK financial services organisations surveyed)

Section 1: Cloud adoption concepts

This section introduces some key cloud adoption terms and concepts that include the different services it offers and the shared responsibility model, deployment models, and common journeys to adoption.

Cloud services and responsibility

Cloud services are available in different service models. These vary depending on what the cloud service provider (CSP) offers, and the responsibilities of the customer. Typically, these models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS includes hardware and network infrastructure. Examples of PaaS are operating systems, such as Windows and Unix. SaaS are usually applications that are ready to be used by the customer, such as Customer Relationship Management (CRM) and email applications.

A clear Shared Responsibility Model should be in place to ensure roles and responsibilities are clearly understood and defined. This includes what controls are managed in the financial institution (FI) and what controls are the responsibility of the CSP. An example of this model is outlined in Figure 2 below.

Shared Responsibility Model

The **Shared Responsibility Matrix** provides a useful conceptual model describing the division of the responsibilities between the cloud service provider and the customer. As seen in the diagram, the level of control and responsibility held by the customer increases, starting with SaaS to PaaS to IaaS. Each service defines what responsibilities are held by the CSP and the customer.

There are 3 types of service models that CSPs usually offer:

- **Software as a Service (SaaS):** provides software over a network while the physical environment is handled by the host e.g. Microsoft 365, G-Suite applications.
- **Platform as a Service (PaaS):** provides a computing platform over a network while the environment is also provided by the host e.g. Windows SQL Library.
- **Infrastructure as a Service (IaaS):** provides a virtual computer structure where the host supplies the hardware and the customer controls the operating system e.g. Azure virtual machines.

Despite the three different service models provided with varying levels of responsibilities, CSPs will always maintain security of the virtualisation layer, physical hosts, network and datacenter.

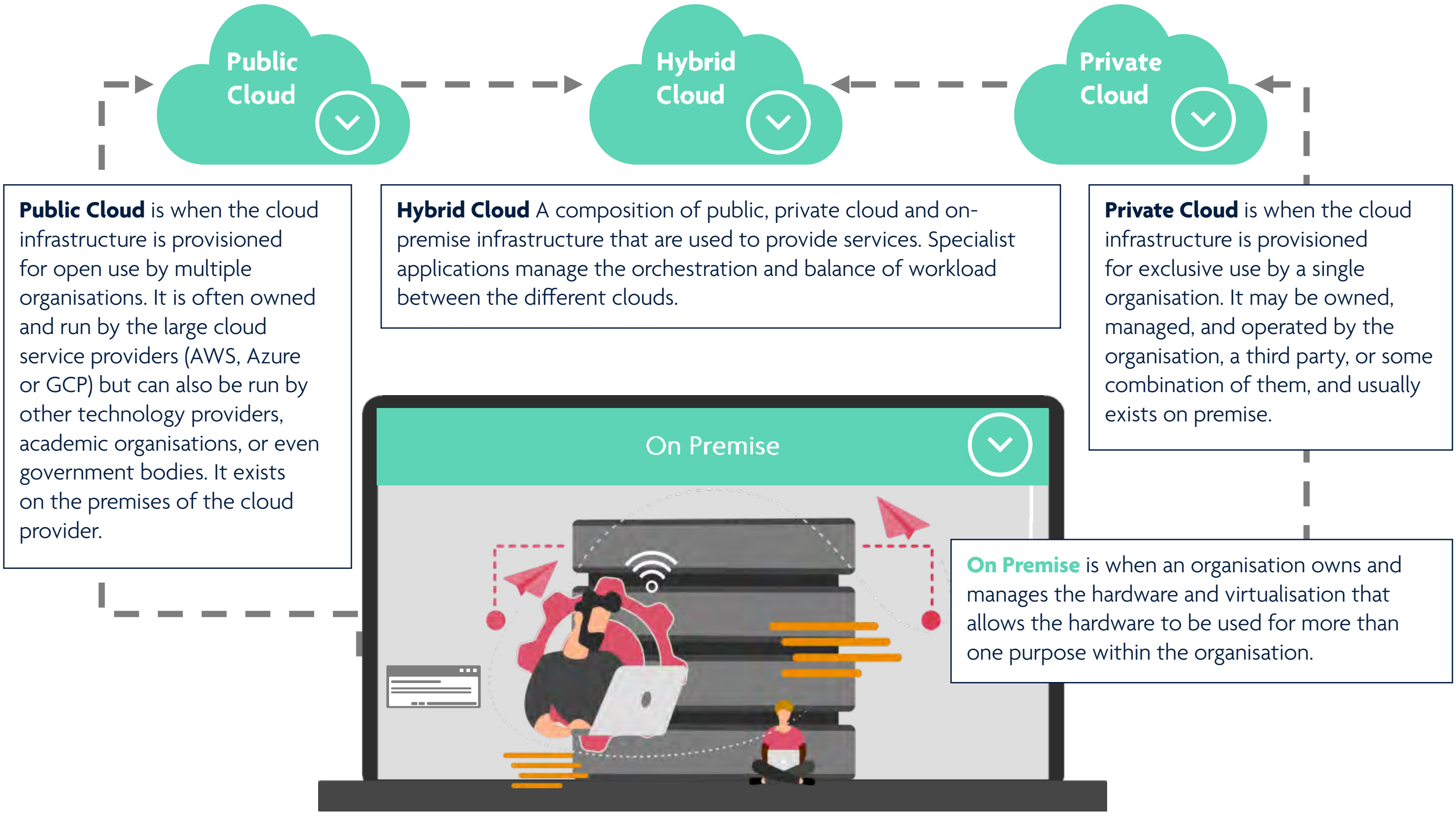
Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟩	🟩	🟩	🟩
Devices (Mobile and PCs)	🟩	🟩	🟩	🟩
Accounts and identities	🟩	🟩	🟩	🟩
Identity and directory infrastructure	◩	◩	🟩	🟩
Applications	■	◩	🟩	🟩
Network controls	■	◩	🟩	🟩
Operating system	■	■	🟩	🟩
Physical hosts	■	■	■	🟩
Physical network	■	■	■	🟩
Physical data centre	■	■	■	🟩

Cloud Service Provider responsibility ◩ Mixed responsibility 🟩 Customer's responsibility

Figure 2 - Cloud shared responsibility model

Deployment models

As depicted in Figure 3, cloud can be deployed in an organisation via various models such as a private cloud, public cloud or hybrid. In private cloud, computing services are consumed from IT infrastructure that is either housed within the firm's own data centre or that of a third party. This IT infrastructure is not shared with other organisations. In public cloud, cloud services and infrastructure are offered by a third party (the CSP) over the public internet, making them available to multiple organisations on demand on a pay-per-use consumption model. Hybrid models are a combination of private and public cloud models.



Public Cloud is when the cloud infrastructure is provisioned for open use by multiple organisations. It is often owned and run by the large cloud service providers (AWS, Azure or GCP) but can also be run by other technology providers, academic organisations, or even government bodies. It exists on the premises of the cloud provider.

Hybrid Cloud A composition of public, private cloud and on-premise infrastructure that are used to provide services. Specialist applications manage the orchestration and balance of workload between the different clouds.

Private Cloud is when 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 usually exists on premise.

On Premise is when an organisation owns and manages the hardware and virtualisation that allows the hardware to be used for more than one purpose within the organisation.

Figure 3 - Cloud deployment models

Adoption journeys

As depicted in Figure 4, factors such as organisational culture, skill sets and roles, and IT spend tend to determine where organisations are in their adoption journey. As organisations navigate through each stage of the cloud adoption journey, from initial adoption to becoming a truly cloud-native organisation, it is essential that they consider the different risk profiles that this presents and what model, or combination of models, is most appropriate for their organisational needs.

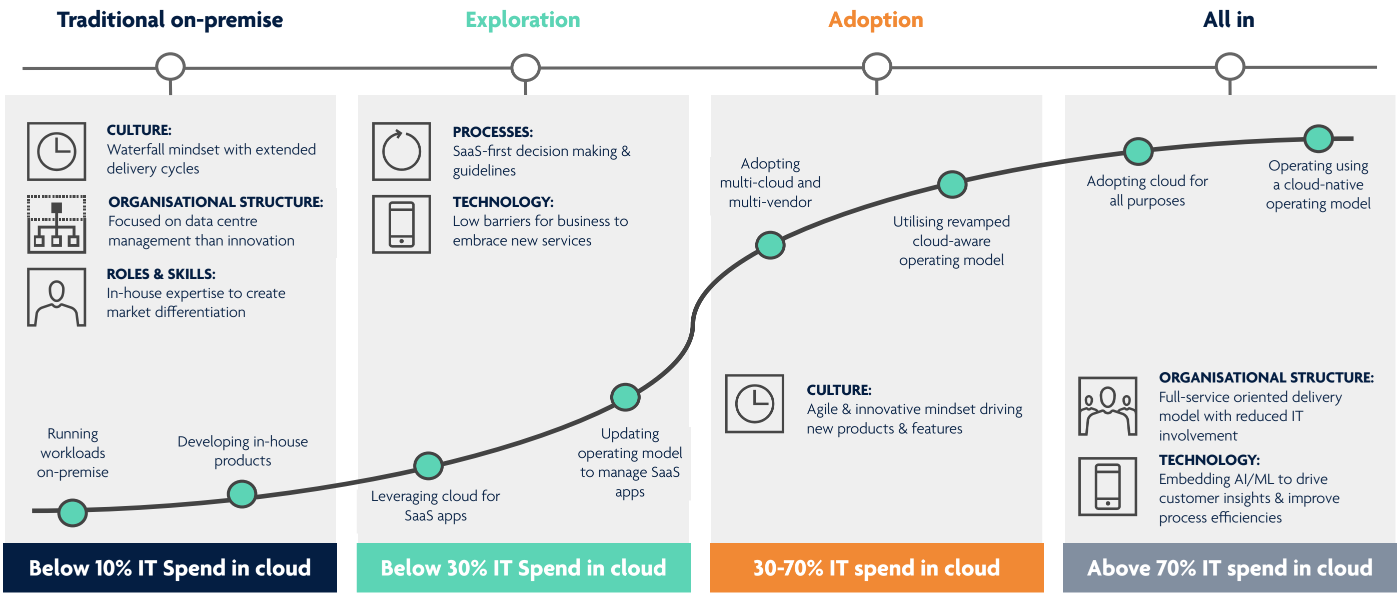

Traditional on-premise
Exploration
Adoption
All in
CULTURE:
Waterfall mindset with extended delivery cycles
ORGANISATIONAL STRUCTURE:
Focused on data centre management than innovation
ROLES & SKILLS:
In-house expertise to create market differentiation
Running workloads on-premise
Developing in-house products
PROCESSES:
SaaS-first decision making & guidelines
TECHNOLOGY:
Low barriers for business to embrace new services
Leveraging cloud for SaaS apps
Updating operating model to manage SaaS apps
Adopting multi-cloud and multi-vendor
Utilising revamped cloud-aware operating model
CULTURE:
Agile & innovative mindset driving new products & features
Adopting cloud for all purposes
Operating using a cloud-native operating model
ORGANISATIONAL STRUCTURE:
Full-service oriented delivery model with reduced IT involvement
TECHNOLOGY:
Embedding AI/ML to drive customer insights & improve process efficiencies
Below 10% IT Spend in cloud
Below 30% IT Spend in cloud
30-70% IT spend in cloud
Above 70% IT spend in cloud

Figure 4 - Cloud adoption strategy journey

Cloud adoption includes taking into consideration the various service and deployment models outlined above, as well as deciding the best way to move on premise applications to cloud, the possibility to build cloud-native applications and to acquire SaaS solutions. It requires preparation, readiness assessment and planning. It is key to first understand the organisation's overall business and technology strategies. Based on these strategies, organisations need to assess their current 'on-prem workloads' and determine the best course of action to realise the benefits of strategic cloud services and solutions.

There are different options and routes for cloud adoption. For example, "lift-and-shift", re-factoring or re-architecting of current applications, native cloud developments and hybrid approaches. The strategy to follow will depend on various factors, including the overall business and technology strategy, complexity of current workloads, cost-benefit analysis, regulatory expectations and the need to modernise and optimise applications, to name but a few.

There is no single answer to what strategy should be followed. Different strategies have their own drivers, depending on business case and technology considerations. For example, lift-and-shift may be useful to reduce the data center footprint and better segment IT networks as a quick win, however it is not a sustainable long-term strategy because there is nothing changing here other than moving legacy complexities and inherent architectural vulnerabilities to a different environment. This strategy will also not help to unlock the full benefits the CSP has to provide. It may also increase risk exposure in the early phases of cloud adoption if agile development practices are being used in a less well-defined and monitored cloud environment. Re-factoring has benefits in terms of better embedding more sophisticated cloud-native cyber defences but this approach may not always be suitable from a business perspective (e.g. a life insurance application that only keeps policy information and a log of records until the product is sold to someone else). It may also be hindered by requirements to maintain a go-live backup in a different cloud environment or to design your applications to be fully portable.

Section 2: Understanding key cloud benefits and misconceptions (two sides of the same coin)

This section highlights some of the main cloud security and resilience benefits and also the misconceptions.

Improved security and resilience but regulatory compliance considerations

Cloud providers implement security by design, and sometimes by default, for their platforms and the data they process, such as authentication, access control and encryption. These capabilities also tend to be continuously enhanced and improved, and transparent to the customer's experience (such as removing remote access by default to cloud storage). Organisations can then add security measures to tighten access to sensitive information in line with their specific business needs. CSPs offer robust and resilient architectures, for example by implementing multiple cloud geographic 'regions' and 'zones' with high availability configurations. This means that financial institutions can reduce their time and effort on fixing potential issues relating to downtime. They can architect highly resilient solutions to support critical workloads in the cloud. For example, financial institutions building or enhancing real-time payment systems for customers to make secure and reliable transactions can architect and deploy these systems across multiple time zones to achieve high availability.

While resilient by design, the global nature of cloud infrastructure may give rise to concerns about compliance with data sovereignty requirements. Financial institutions need to consider the compliance and regulatory requirements relating to the location of their data, and the regions the data is transferred to and stored or processed. For example, they can determine what geographical regions to use for particular applications and data that cannot be physically located outside a particular region. This can be done by restricting the access to regions in the configuration and security of the cloud services and infrastructure, and also tagging resources with data classifications which limit where the data can be processed. They also need to consider potential restrictions in some regions which impact availability configurations. In the same vein, authorities need to consider the resilience trade offs they may be forcing firms to making through localisation policies and considerations.

The general consensus is that adopting the public cloud has increased organisations' operational resilience capabilities compared to on-premise systems – two-thirds of UK Finance members surveyed agreed with this.

Multi-cloud does not always equal more resilience

There is currently a trend to consider multi-cloud arrangements to improve resilience, in addition to leveraging the benefits of different CSP services and features. Around 50 per cent of UK Finance members surveyed mentioned deploying a multi-cloud strategy to achieve their business goals and objectives; of these, 100 per cent considered it to achieve operational resilience benefits.

While a multi cloud approach is sometimes discussed as a means of addressing concentration risk, the benefits that multi-cloud approach has to offer do not fully address concerns over perceived concentration risk. A market approach to addressing this risk at a systemic level is to create an innovation-friendly climate that helps emerging CSPs challenge the dominance of established players. Other approaches to mitigating this risk include well-constructed exit strategies and plans, and architecting applications to be portable, deployed in an automated and standardised manner, and resilient by design. However, there are limits to what portability can achieve and it should not be expected to serve as a short-term solution to a major outage at a public cloud provider.[1]

[1] https://www.afme.eu/publications/reports/details/Building-Resilience-in-the-Cloud

A hybrid approach – where firms deploy public cloud strategies for certain workloads but also maintain in-house data centres – remains perhaps the most common in the finance industry although there are consistent shifts towards the migration out of traditional data centres. The majority of UK Finance members who took part in our survey remain focused on the hybrid approach – a combination of public cloud and on-premise data centres. A hybrid strategy is essential for firms that want to maintain certain data and workloads on premise for a variety of internal reasons.

In summary the benefits and requirements for a multi-cloud strategy should be assessed against concrete business needs and clearly articulated risk analysis.

Simplification

According to PwC's CEO Survey[2], cyber security is a top concern for CEOs. Core to addressing this concern is the simplification of IT, which addresses the root cause of the problem in making an organisation 'securable'[3]. Cloud can be catalyst for simplification through automation, modernisation and standardisation. A byproduct of simplification is also cost optimisation and predictability and cloud can be seen loud is a catalyst for simplification through automation, modernisation and standardisation.

Most financial institiutions' technology architecture is made up of layers of legacy systems. This architecture creates multiple constraints on flexibility and represents an ever-expanding dimension of complexity. By contrast, many 'digital native' companies who have more recently entered the market have a simplicity advantage. These companies are built 'digital' from the ground-up, using more recent generations of IT, standards and techniques meant to create increased interoperability across systems. Legacy structures are often riddled with open 'seams' and soft connections that can be exploited by attackers, whose capacity to infiltrate sprawling systems has grown. The pressures on these legacy structures have intensified as companies have pushed their current IT to keep pace with the digital natives.

To help manage the complexity problem, cloud provides capabilities to help engineer a more simple technology estate. This includes greater control to the business in developing and maintaining technology solutions. There is less need for technical teams to install and configure basic solution components in order to implement a functioning 'workload' (a collection of resources and code that delivers business value, such as a customer-facing application or a back-end process)[4]. There are various cloud components and services that can be used with minimal adjustments to meet business changes and market. They also offer pattern-based architecture models that can be reused, allowing flexible and efficient implementation of repeatable functions and processes. In fact, among UK Finance members surveyed an overwhelming 85 per cent of respondents said that migrating to public cloud had helped reduce certain legacy risks compared to the on-premises systems.

Addressing misconceptions

A key root cause of cloud misconceptions is people's understanding, their cloud competencies, and associated risk management experience. There is a shortage of people with cloud skills and expertise in the market. For example, over 50 per cent of UK Finance survey respondents mentioned a lack of in-house expertise building AI/ML models in the cloud as one of their key challenges. Organisations should consider training their existing engineers and risk analysts in cloud technologies — but this cannot be done in isolation. Trial and error can be an expensive way to learn, and will take much more time than working with someone who already knows the 'ins and outs' of the cloud – one reason why only six percent of business and tech/security executives see their organisations fully realising benefits from cloud adoption, as mentioned previously. Partnering with an organisation or individual with cloud migration/modernisation and management experience and certifications can be an expedient way to achieve business goals and objectives and manage risk.

[2] **https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021.html**

[3] **https://www.pwc.com/gx/en/issues/reinventing-the-future/take-on-tomorrow/simplifying-cybersecurity.html**

[4] **https://docs.aws.amazon.com/wellarchitected/latest/userguide/workloads.html**

Section 3: Cloud risk management

This section addresses some core risk management topics of cloud adoption. These include its difference to traditional outsourcing, differences to traditional technology risk management, as well as regulatory compliance and assurance considerations.

Traditional outsourcing vs cloud computing

Financial institutions are under increasing pressure to reduce costs, become more agile in responding to customer requirements and meet emerging regulatory expectations. Many have tried to address these issues by moving to traditional Information and Communication Technology (ICT) outsourcing to reduce costs and achieve more efficiency. However, this model has become increasingly challenging, due to the difficulties in managing the ICT outsourcing contracts and services to meet financial institutions' technical and business requirements. Additionally, legacy infrastructure and closed solutions on financial institutions premises or in ICT outsourcing arrangements are typically not cost effective and flexible enough to address these challenges. They are usually burdensome and expensive to maintain and update to meet increasing and complex customer demands and regulations. Financial institutions are increasingly adopting cloud services to address these challenges. In fact, only one UK Finance survey respondent said they do not directly use any cloud-based solutions. This tendency includes migrating critical workloads to the public cloud or building cloud native applications to gain the benefits of cloud infrastructure and services, such as flexibility, scalability, efficiency and cost optimisation. Cloud adoption is an opportunity for firms to become more agile, secure and resilient, provided they follow good practices in line with modern technology approaches and up to date control frameworks adapted to cloud environments.

Traditional cloud technology outsourcing tends to rely on a multi-tenancy model whereby multiple customers may access a single shared application and infrastructure with little to sometimes no isolation between customer sessions and data. This reduces the ability to contain operational issues to one customer's context. A good example of this is Cloud Hopper[5] where a nation state threat actor was able to move between different customer instances via a Managed Service Provider's shared infrastructure. Depending on the cloud deployment model used by the financial institution, appropriate implementation strategies and risk management activities and controls will need to be implemented. For example, in public cloud, if firms use a cloud storage service and they want to port the data to another CSP and exit that relationship, what assurances will they receive from the CSP that their data is destroyed and / or not readable to an insider or other malicious actor in future? Some organisations are ensuring that, as part of implementing these services, they have the ability to encrypt sensitive data and destroy the keys so that the data is not retrievable (also known as cryptographic key shredding). For hybrid cloud, the organisation will need to develop and manage controls across multiple environments that could increase complexity and effort if not orchestrated from a single or central control plane.

While multi-tenancy still exists (i.e. at the infrastructure layer) cloud infrastructure and tools are designed to take advantage of the latest technologies and architectures to improve service instance isolation per customer, service independency, services on-demand, and service scalability and elasticity. However, these new features can present emerging challenges to risk management that CSPs must support financial institutions with. Legacy governance structures, processes and controls need to adapt to this new reality. Firms need to modernise their technology systems and adapt their governance and controls while complying with a changing regulatory landscape that is increasing its focus on cloud. This adaptation includes adjusting organisational culture, capability and training to leverage the knowledge of current legacy systems, developing transition strategies and implementing strong foundation architecture and landing zones (reference architecture) and development 'guard rails'. This should include the right balance between control and agility. 85 per cent of UK Finance members surveyed agree they are adapting to this new way of outsourcing and growing comfortable that CSPs understand applicable outsourcing requirements.

[5] '**Operation Cloud Hopper**', joint report published by PwC UK and BAE Systems in April 2017

Organisations need to have a thorough understanding of how important business services are supported by cloud infrastructure, applications and services. This includes, for example, mapping business services to cloud components, and third parties' cloud components; assessing how disruptions of such components may affect the delivery of the service; and having a disaster recovery plan in place (highlighted by a recent cloud edge provider outage). Supply chain complexity is likely to increase as financial institutions and wider digital ecosystems move towards cloud computing. Automatically inventorying, mapping dependencies, and developing recovery and contingency plans in an efficient manner will become correspondingly more important.

Risk management in/on the cloud

In order to manage security and resilience risks effectively, organisations need to demonstrate cyber resilience against the various threat scenarios in cloud environments and recognise the differences with traditional technology risk management. The approach should consider the assessment of capabilities that reduce the likelihood and impact of threats to CSPs and to cloud workloads, through appropriately designed, implemented and monitored capabilities. These capabilities should include functions that identify cloud technology assets and data, protect these assets from threats, and detect, respond and recover to and from events and incidents. In addition, organisations should consider cloud and broader security and resilience standards based on regulatory expectations (UK[6] and Europe[7]), and industry good practices and frameworks (expanded on below).

Risk management over CSPs and cloud workloads is different to that of traditional technology risk management in several ways.

Attack surface management

Cloud's attack surface, while conceptually similar to traditional technology architecture (people, user devices and endpoints, application and their source code, supporting infrastructure), has some common components that require more focused risk mitigation strategies.

For example, Application Programming Interfaces or APIs (a standard way of interoperability between cloud, inter-cloud and non-cloud services), require robust authentication, authorisation, data security, vulnerability management and logging and monitoring. In one instance, a financial institution's mobile banking app was compromised when the bank's former third party data analytics development team's API key was exposed which allowed a malicious attacker to extract personal data from their systems[8]. OWASP provides a useful cheat sheet on API security[9] that can be used by developers to make sure fundamental API controls are considered as part of the development process.

Another area is cryptography and cryptographic key management applications and infrastructure. Cryptography protects the confidentiality and integrity of data and information at rest, in transport, and in use (e.g. on and between public cloud workloads and shared infrastructure) by using keys and encryption algorithms to scramble the information. For the data to be protected the private or symmetric keys must be only known by the authorised users. If these keys are lost or exposed in any computer environment the data they protect is no longer secure. Specialist devices known as Security Modules are used to provide secure key storage and to ensure that attackers cannot easily discover these keys. Securing these keys against attack techniques in the cloud and applications is a challenge to solve. Cyber criminals and hostile states go to extreme lengths and develop techniques to discover and extract encryption keys due to the high value of information they usually protect. Knowing that cloud keys are an attractive target to these threat actors is a risk appetite decision all organisations will need to make when using public cloud: 1) Use the cloud's cryptographic key management system, or 2) Procure and manage their own. It is important to note that whilst cryptographic keys can protect organisations' data and provide security, confidentiality and integrity, if they lose the keys they lose the data so backups are an important consideration. Cloud key management systems do not support key backups by default so it is something that organisations need to engineer prior to implementation.

[6] https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

[7] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

[8] https://www.bankinfosecurity.com/dave-mobile-banking-app-breach-exposes-3-million-accounts-a-14708

[9] https://owasp.org/www-project-api-security/

Another important area is containerisation, which is a modern technology that enables applications to maximise infrastructure costs (via virtualisation) through a lightweight design, have greater isolation for security, improved resilience and maintenance, and, when architected correctly, have the ability to run on any infrastructure. However, this is dependent on design tradeoffs. Containerisation to the point of moving between infrastructure may mean not taking advantage of specific or unique capabilities of the infrastructure you are deploying on and could have a long-term effect on the ability to maiximise security and resilience. Furthermore, these containers introduce another attack surface that needs to be inventoried and their vulnerabilities managed, and the container estate can become complex to manage and orchestrate unless well curated. Capturing sufficient forensic information to support audit requirements and incident response from these dynamic workloads is also challenging. A few emerging vendors are developing forensic tools that can support these requirements in addition to coverage provided by native cloud logging solutions.

Secure and resilient by design

With the increased ability for cloud service providers to build cloud services, supported by a plethora of agile tools, managing change is difficult for security and resilience teams to keep pace with. Several important secure and resilience-by-design capabilities must be established as part of adoption:

- The first is **good inventory management**. This starts by having a single inventory of CSP billing accounts, and for each service consumed / workload created a dynamic inventory that links these services to organisational business processes. This can be supported through designing identity management and role-based access in a way that allows organisations to link business features to cloud services as and when they are created and destroyed through resource tagging.
- The second capability is **build management**. Most 'on premise' environments suffer from a plethora of different technology builds that require expensive and manually intensive activity to maintain, change and manage vulnerabilities. Cloud build tools allow development and engineering teams to create secure and scalable infrastructure that can be templated to be deployed and redeployed at pace – e.g. following a security issue with a specific workload – without the need to manually contain and recover each individual system affected ('immutable workloads' – technology that organisations can deploy and redeploy in a repeatable and efficient manner when an issue occurs or when a vulnerability needs to be mitigated at scale).
- Fundamentally, **adopting an open source approach** can offer not only greater choice, but a more robust approach to resilience, compliance, and business continuity. Provider adherence with the recognised portability codes of conduct, such as SWIPO[10], should also be duly considered. However, portability should be treated as a means rather than an end: it is a tool to support exit plans, rather than an essential feature of all cloud services.
- Migrating / adopting the cloud means **transforming** how organisations think about, deploy, and manage infrastructure. When servers, racks, and data centers are managed for organisations in the cloud, their code becomes their infrastructure. When organisations deploy **infrastructure as code**, they can integrate their security and resilience policies directly in the code (**policy as code**), making security and resilience central to both the organisation's development process and to any software that it develops, and also helping to minimise risks.
- Finally, **cloud development** as already covered increases the pace of releasing new features which need to be managed. To address this challenge, organisations need to adopt the 'shift left' principle by training their staff to do the right thing (i.e. secure coding), trusting them to operate through tools that can help them identify weaknesses during the development process, and by integrating security and resilience issues identified into the business requirements backlog.

Control governance and monitoring

As outlined in previous sections, the shared responsibility model means that control implementations differ depending on the type of model adopted. For example, in a SaaS model building strong access controls would be a focus, while an IaaS model would require building not only access controls but also vulnerability management and threat detection and response. As such, it is important that both third-party security and applications/infrastructure security risk teams

[10] **https://swipo.eu/**

assess their CSPs and individual workload security appropriately and accordingly, attributing ownership to the different models and control instances, and establishing good governance through RACIs, internal procedures and third-party contract schedules (where third parties are used to build and maintain cloud environments).

Many leading financial institutions assess CSPs against a common control framework, typically based on or aligned to the NCSC cloud security principles[11], the Cyber Security Alliance CCM[12], NIST Cyber Security Framework, the Financial Sector Profile[13] and COBIT[14]. Then, application and infrastructure teams would perform assessments of cloud services and workloads run on CSP infrastructure using a combination of infrastructure control templates (using CIS or vendor guidance) and application threat modelling (leveraging OWASP[15] and MITRE Att&ck[16]). The emerging Continuous Control Monitoring capabilities in industry (supported through native CSP tools) are also a vital service for the dynamic nature of cloud, and as part of developing control designs organisations should ensure measurability and automation of data collection on control operations.

Regulation, compliance, and assurance

The majority of UK Finance members surveyed highlighted certain regulatory and compliance challenges such as data residence and localisation concerns post-Brexit; lack of harmonisation in supervisory practices depending on the CSPs; complex supervisor review and response processes; and political and regulatory uncertainty over EU/outside UK operations (such as relevant organisations adherence to the EU's Digital Operational Resilience Act (DORA)). More recently, the Financial Policy Committee (FPC) in the July 2021 edition of the Financial Stability Report[17] called out the issues raised by critical third parties, including CSPs and the potential risks they pose to financial stability. The FPC in its October 2021 financial policy summary and record further highlighted the need for additional policy measures to mitigate financial stability issues identified in this area.

Organisations should work with their business partners, the CSPs in this case, to scan for these challenges and plan together as they move along their cloud adoption journey. Regulators should also work with firms to develop a more standardised approach which could include developing approved platforms and architectures to support adoption. A potential outcome with collaboration such as this can be seen with CSPs increasing the Availability SLAs of their services to serve the needs of their customers. In fact, 76 per cent of the survey respondents mentioned CSPs supporting them in meeting their compliance obligations.

For organisations to obtain assurance on control effectiveness to address regulatory and compliance requirements, they need to take into consideration who is responsible for designing and operating the key controls. An example of this is the development of the cloud security initiative[18] for the financial sector by the Cyber Risk Institute (CRI) in collaboration with the Cloud Security Alliance (CSA). The purpose of this initiative is to work with the cloud service providers and the financial institution to develop a mutually beneficial framework for assessing security responsibilities and cyber risk. There are various mechanisms to obtain assurance over controls by the CSPs, such as assurance reports (e.g. SOC 2) and certifications (e.g. ISO, CSA STAR) made available by the CSPs and the possibility to conduct audits by exercising the right-to-audit contractual arrangements.

[11] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

[12] https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[13] https://cyberriskinstitute.org/the-profile/

[14] https://www.isaca.org/resources/cobit

[15] https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf

[16] https://attack.mitre.org/matrices/enterprise/cloud/

[17] https://www.bankofengland.co.uk/financial-stability-report/2021/july-2021

[18] https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

Conclusion

This paper has outlined the benefits of cloud adoption, including greater security and resilience by default, and if well engineered the foundations of a simpler and more manageable technology estate. Highlighted within this paper are also some common misconceptions and risks, and how they can be mitigated with appropriate strategies that differ from traditional outsourcing approaches and technology risk management. Broadly, cloud benefits can outweigh the risks if financial institutions take a considered approach, and our survey suggests that UK Finance members will continue to move along their cloud adoption journeys at pace.

To support these journeys, we would recommend that the regulators and supervisors take the following topics and points into consideration:

GOVERNANCE & TECHNOLOGY

1. Support the different financial institutions and communities based on their stage of the adoption journey (as highlighted in section 1), through working groups and information sharing. This would include building a common body of knowledge on cloud adoption and sharing good practices and approaches.

REGULATION

2. Clarify cloud-specific applicability of risk management guidance, utilising existing frameworks (as highlighted in section 3), that help financial institutions pivot from traditional outsourcing and technology risk management practices towards an enhanced approach that focuses on secure and resilience by design in and on the cloud.

3. Support financial institutions and CSPs with guidance on regulatory expectations for the various types of cloud deployments and common use cases (including data movement) as financial institutions progress in their cloud adoption journey. This can include, for example, key considerations on how institutions can demonstrate compliance with these expectations (e.g. through common control frameworks, acceptable implementation patterns, and in future minimum policy-as-code checklists) and how CSPs can facilitate this.

ECOSYSTEM

4. Support UK financial institutions in joining up their value propositions across markets, helping to stimulate an innovation-friendly climate that helps emerging CSPs challenge the dominance of established players. This would include developing a marketplace, cataloging the business use cases and associated CSP services, and allowing ‘fringe’ CSPs to be rated and to showcase their strengths.

CLOUD RESILIENCE EXPECTATIONS

5. Standardise the principles behind the potential requirement for exit strategies, particularly in the context of cloud outsourcing. This could include clarification of the scenarios in which a firm would be expected to deploy its exit strategy, analysis of impact tolerances based on these services, efficacy of financial institutions’ resilience and recovery capabilities.

6. Support UK financial institutions in shaping the understanding and analysis of concentration risk, working with cloud service providers to enable the development and collaboration on appropriate risk mitigation strategies.

Acknowledgments

Thank you to all the authors and contributors across the industry and professional services.

Oge Udensi
Principal, Cyber and
Third Party Risk
UK Finance

Zelfau Rauof
Analyst, Cyber and Third
Party Risk,
UK Finance

Ksenia Duxfield-Karyakina
Government Affairs & Public Policy,
Senior Manager, Head of Financial
Services Public Policy,
Google Cloud

Nick Godfrey
Director, Office of the CISO,
Google Cloud

Matthew Burns
Cyber Security Director,
Financial Services and
Cyber Transformation
PwC

Horacio Aeberhard
Cloud and IT Resilience
Senior Manager,
Financial Services and
Digital Transformation
PwC

Sivaram Mallampati
Cyber Security Manager,
Financial Services and
Cyber Transformation
PwC

This report is intended to provide general information only and is not intended to be comprehensive or to provide legal, regulatory, financial or other advice to any person. Information contained in this report based on public sources has been assumed to be reliable and no representation or undertaking is made or given as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or any of their respective members, officers, employees or agents shall have any liability to any person arising from or in connection with any use of this report or any information or views contained in this report.