REGULATORY UPDATE - BERLIN SEPTEMBER 2020
Policy note drafted by the Eurofi Secretariat

Cloud services: uptake in the financial sector and policy approach

1. The uptake of cloud in the financial sector is progressing, however there is still scope for further adoption

1.1. Main current cloud operating models

Cloud computing provides remote on-demand access via the web to a shared pool of configurable computing resources (e.g. networks, servers, storage, software applications, analytical tools) offered as standard building blocks by cloud service providers (CSPs) that can be progressively and rapidly provisioned, with no physical interaction with the CSP. Cloud services are usually offered on a pay-per-use basis via a subscription.

There are three main types of cloud services[1]. Software as a Service (SaaS)[2], which offers access to off-the-shelf application software, is the largest cloud service model at present, representing approximately 50% of cloud spending. Infrastructure as a Service (IaaS) providing access to processing and storage capacity and Platform as a Service (PaaS) services[3] providing access to software development and deployment platforms, represent a smaller share of the market. IaaS may nevertheless play an increasing role in the future notably with the development of artificial intelligence (AI) applications, which require significant data storage and processing capacities that can be offered via the cloud. PaaS solutions also offer software components and tools that can help financial institutions to develop and launch more effectively AI solutions. Gartner for example predicts that IaaS will have the fastest growth rate among cloud services through 2021[4].

Cloud services can be provided on-premise for the exclusive use of one organisation or of a community of users. This service known as private cloud[5] is at present the dominant model in the financial sector. But it is the public cloud model[6] (standardised services provided remotely in a highly automated manner and on a large scale to multiple customers) that allows the leveraging of all the potentialities of cloud services, according to CSPs. With public cloud, multiple customers can potentially share the same best-in-class computing resources, analytical capacities, software applications and tools with a secured access to segregated components. Public cloud also provides access to almost unlimited data storage and processing capacities. This type of mutualised service is estimated to represent about 30% of cloud service use in the financial sector, however just 18% of financial services firms said they are broadly implementing IaaS for production applications today for example in a recent survey, compared to 25% of businesses overall, showing a significant margin for progression[7]. There are nevertheless significant differences within the financial sector when comparing new entrants (Fintechs, Insurtechs) and more established players.

1.2. Main industry trends and drivers of cloud services development in the financial sector

The use of cloud services is expected to grow at a fast pace in the financial sector in the coming years with the increasing digitalisation of financial services, the expansion of data driven business models and also with regulations requiring extensive data storage and processing capacities (e.g. MiFID II, FRTB, etc.)[8]. It is likely that new developments supported by technology and data such as artificial intelligence (AI)[9], regtech and suptech[10] and open finance[11] will further drive

[1] Definition adapted from the US National Institute of Standards and Technology (NIST).

[2] Software as a Service (SaaS): offers access (free or paid via a subscription) to off-the-shelf application software from any device with an internet connection and web browser. A suite of applications and processes can also be managed and delivered on the cloud with a Business Process as a Service model (BPaaS)

[3] Infrastructure as a Service (IaaS) provides access to processing power, storage or network services. Platform as a Service (PaaS) provides a computing platform with the relevant application development and deployment environment (i.e. programming languages, tools, databases, resources, etc.) allowing users to develop, test and manage their own applications without building or managing any infrastructure. Users have different levels of control depending on the service level. With IaaS, users have control over storage levels, computing capacity or the access to certain network components. With PaaS, users have control of their own applications that run on the platform and of the platform's configuration settings. And with SaaS, users have control of configuration settings specific to the applications they are using.

[4] Source FSB report on « Third-party dependencies in cloud services" 9/12/2019

[5] Private cloud: the cloud infrastructure is provisioned for exclusive use by a single organisation, that manages the capacity and it may be on or off the premises of this organisation. Community cloud is a variation of the private cloud where the cloud infrastructure is provisioned for exclusive use by a community of organisations or users that have shared needs, manage the capacity together with the CSP and it may also be on or off premises

[6] Public cloud: the cloud infrastructure is provisioned for open use by multiple organisations concurrently and is run on the premises of the CSP that also manages capacity

[7] Source "Financial services companies must embrace the cloud" February 2019 – Information Age. A survey published in November 2019 by AFME also indicates that 2/3 of AFME members estimated that 1 to 10% of their bank's current workload was using public cloud.

[8] For example FRTB (the Fundamental Review of the Trading Book) applying to financial intermediaries operating in the capital markets requires an eightfold increase of IT infrastructure spending by some institutions to comply with the regulation, due to the enhanced risk modelling and the number and frequency of calculations required, as well as the amount of data involved. Source Eurofi – Summary of the Bucharest High Level Seminar April 2020

[9] AI applications for enhancing automation or developing more personalised services require extensive computing power, specific chips, data management capacities and analytical tools that can all be accessed via the cloud

cloud adoption in the financial sector in the coming years. Some projections show that the addressable cloud market in Europe for financial services could double or triple between 2019 and 2023[12].

However most financial institutions are still at an early stage in their implementation of public cloud services with the exception of Fintechs, whose services are usually built on public cloud platforms from the outset because of the scalability and flexibility they offer[13]. Further, 70% of financial companies at the international level indeed reported in a recent survey[14] that they were still at the "initial or trial and testing stage" of their cloud development. While traditional financial institutions have been early adopters of private cloud solutions, their migration to public cloud is still relatively limited. They are so far mainly using public cloud services for processes that are not material or do not require the exchange of sensitive business data[15] and in functions that are not tightly tied to legacy IT systems.

The adoption of public cloud-based infrastructures is nevertheless progressing, with financial institutions starting to use the public cloud to manage and process large volumes of data related to core financial activities[16]. This allows them to accelerate the digitalisation of their services and also develop and launch new products in a faster and more flexible way.

Some emerging trends, such as the development of edge computing and IoT (internet of things) data generated by smart connected objects may also create new dynamics in the market in the future with more data expected to be created and processed where the data is collected and therefore outside data centres and cloud[17]. It is however expected that cloud services will continue to play a strong role in this context since cloud computing will be needed to store IoT data. The specific impacts of these evolutions for financial services data also need to be further assessed.

The Covid crisis has also prompted Financial Services organizations to reconsider how they see their IT infrastructure needs going forward. Many have resorted to the cloud to allow their collaborators and clients to continue to operate without disruptions during lockdowns[18] and this trend, leveraging the scalability and flexibility of the cloud, is due to continue.

2. Benefits and risks associated with cloud services and barriers to adoption

2.1. Potential benefits of public cloud computing

Although there are benefits derived from using private cloud services (increased flexibility of computing resources, improved scalability, easier collaboration and synchronisation within firms through data sharing…), the advantages of migrating to the cloud are usually associated mostly with public cloud services.

Some institutions combine the use of public and private cloud (known as hybrid cloud) and multiple CSPs can be used in cloud architectures(known as multi-cloud).

Public cloud services indeed facilitate access to best-in class computing, security and software resources, through a mutualisation across a large number of customers. Due to its scalable and pay-as-you-go model, public cloud also offers benefits in terms of cost efficiency, flexibility and agility that can support the progressive digital transformation of financial firms. Public cloud services also provide benefits in terms of risk mitigation with the shared benefit of increased resiliency[19], a high level of automation and a greater uniformity of the IT environment than on-premise IT. An additional benefit is the possibility of raising the efficiency and scale of regulatory reporting, compliance and internal risk processes and also facilitating interaction with financial supervisors.

Cloud platforms also facilitate the development and implementation[20] of new technologies such as AI[21] or DLT[22] that contribute to improving innovation, efficiency and risk mitigation, and that may be difficult to implement in a traditional IT environment. The public cloud also offers greater opportunities to leverage large quantities of data (e.g. for developing and training AI based systems). Outsourcing to

[10] Increasing compliance, reporting and risk management obligations imposed by financial regulations, leading to an expansion of data storage and processing needs, are a further driver of cloud services.

[11] Open finance concepts that support the development of new distribution channels and new financial services (e.g. account aggregation, financial planning) leverage cloud infrastructures e.g. to connect different accounts or aggregate data.

[12] Source: market forecast made by some CSPs in 2019. An earlier report on the finance cloud market predicted a CAGR of 24% by 2021 globally (Source "Cloud adoption in the financial services industry" – Cloud technology partners).

[13] Public cloud services are the basis of the IT architectures of all the fintechs that have developed new business models with data at the centre of their value proposition, which tend to be "cloud-native" players.

[14] Source FSB report « Third-party dependencies in cloud services" 9/12/2019

[15] i.e. such as human resources, project management, communication tools, CRM, etc.

[16] e.g. for activities related to transactions or end-of-day batch processing

[17] According to statistics quoted by the Commission in its White Paper on AI, while today 80% of data processing and analysis takes place in data centres and centralised computing facilities including cloud platforms, and 20% in smart connected objects, such as cars, home appliances or manufacturing robots, and in computing facilities close to the user ("edge computing"), these proportions are set to change markedly by 2025. Source EU Commission White Paper on AI - February 2020. Some market observers however also question this forecast given the early days of edge computing in particular.

[18] As an example, as lockdowns around the world forced hundreds of thousands of workers in the FS sector to stay in their homes, banks and other financial institutions leveraged cloud services to allow those workers to continue to work from their homes, keeping the financial system going. This was only possible given the scalability and flexibility provided by the public cloud.

[19] Resiliency features used by CSPs include: geographical redundancy of data centres, back-ups, cyber-security systems, compliance programmes, automated security controls. Workload mobility features include: containerisation of workloads, open source IT environments…

[20] Cloud services supply access to development and deployment platforms, software components, etc…that are used for developing AI systems and software.

[21] For example AI applications contribute to providing innovative products (based e.g. on predictive analytics or personalisation), increasing automation and also mitigating money laundering, fraud or cyber-risks.

[22] Distributed Ledger Technology (DLT) applications can contribute to improving the efficiency and safety of transactions.

public cloud platforms moreover allows firms to redirect internal resources previously focused on the administration of internal IT platforms, towards more added value activities and services that may enhance innovation and risk mitigation efforts.

Adopting public cloud at scale in order to reap the full benefits it may provide, nevertheless requires that financial firms adapt their operating models and internal processes to the new potentialities of the cloud, rather than simply replicating existing workloads in a different cloud-based environment, which requires a holistic approach to cloud. This involves adapting operational processes in order to embed the interaction with third-party CSPs, downsizing legacy IT platforms and leveraging the full range of cloud services when appropriate (beyond IaaS, which usually involves replicating current IT infrastructures and applications in a different environment).

2.2. Barriers to the wider adoption of public cloud services

Financial institutions, particularly incumbent firms, face a number of challenges and barriers when migrating workloads to the public cloud.

There are firstly operational issues. The existence of legacy IT infrastructures within financial firms and their interconnection is a first barrier to the adoption of more flexible pay-per-use services. The changes usually needed in terms of IT skills to implement outsourced cloud-based solutions are another challenge, together with cultural change and trust issues.

Secondly, a risk of regulatory and supervisory fragmentation of cloud arrangements subsists in the EU, although much progress has been made thanks to the publication by the European Supervisory Authorities (ESAs) of cloud outsourcing guidelines applying to the different sectors of finance (see detail in Section 3). Nonetheless, these guidelines may be interpreted differently among the National Competent Authorities (NCAs)[23] , since they are not underpinned by a European regulation and there may be differences in their application at the national level.

Legal and extra-territoriality issues related to the data stored in the cloud may also hinder the wide adoption of public cloud services in Europe. Firstly, while EU level rules applying to data such as the GDPR define common requirements, variations remain at the Member State level in the way some data rules are interpreted. Secondly, data location requirements that exist in certain countries and which are designed to increase the safety of domestic data may also be a barrier to the adoption of public cloud at scale across the EU, since they limit the possibility to shift data from one data centre to another, if needed. In addition, data location requirements may vary across jurisdictions, adding complexity[24]. Thirdly, the cross-border nature of CSPs also exposes them to potential legal requirements imposed by their (third-country) home authorities. One example that has often been put forward is the Clarifying Lawful Overseas Use of Data Act or CLOUD Act adopted in 2018, which provides US government agencies with rights to request public cloud data managed by CSPs following a due legal process, even when the servers containing the data are abroad. In addition, the CLOUD Act is applicable to any foreign company with an office or subsidiary in the US[25]. These rights under the Cloud Act perceived as a possible threat or element of uncertainty by some European stakeholders (particularly firms that handle a great deal of sensitive data) have triggered requests for greater data protection and sovereignty (i.e. control over data) in a context where the main CSPs are based in the US and China, and notably for non-personal data which is not covered by GDPR. US CSPs however stress that the Cloud Act is not a right to directly access the data held by CSPs, but to request data, and that practically all current requests concern criminal investigations about individuals, to whom requests are forwarded by the CSP[26].

2.3. Potential risks associated with cloud services

Potential future financial stability risks due to the third-party dependencies created by outsourcing to CSPs and the concentration of the CSP market[27] were addressed by the FSB[28], in addition to more traditional business continuity issues, in a context where the scope of activities and processes delegated to CSPs is potentially increasing. These challenges could be amplified by vendor lock-in issues (e.g. due to specific contractual terms) or workload or data portability limitations (e.g. due to differing technical features or terms of service). CSPs however point out that no specific signs of fragility have been evidenced so far e.g. throughout the Covid crisis. The multi-cloud and hybrid architectures increasingly adopted by financial institutions and the resiliency and workload mobility[29] features put in place by CSPs, as well as open source approaches, could also contribute to mitigating these risks. These solutions may however be challenging to implement for certain financial institutions as they require managing several CSPs offering potentially different contractual terms and technical features.

---

[23] There may also be different interpretations of certain criteria impacting the way they are applied

[24] This also makes it more difficult to leverage global risk management and compliance programmes proposed by CSPs Source AFME report on The adoption of public cloud computing in capital markets (Nov 2019) and FSB report on Third-party dependencies in cloud services – December 2019

[25] The CLOUD Act applies to all electronic communication service or remote computing service providers that are subject to U.S. jurisdiction (and not only to US companies), including email providers, telecom companies, social media sites, and cloud providers, whether they are established in the United States or in another country. This means any foreign company with an office or subsidiary in the United States is subject to the CLOUD Act.

[26] US-based CSPs emphasize that data regarding the number of requests and the responses from US CSPs show that, in practice, little has changed since the instruction of the Cloud Act in 2018. Practically all requests from the US authorities concern individuals faced with criminal accusations such as drug trafficking (and not enterprises handling sensitive data), which was the original reason for implementing the Cloud Act. CSPs also stress that they never access customer data directly without the consent of the customer concerned and that direct access is only performed for maintenance reasons and is tracked in a transparent way and only concerns maintenance. Possible requests from the US authorities are redirected by the CSP to the individual concerned.

[27] The public cloud services market, being a scale business, is concentrated, with the top five public CSPs representing over 75% of the total public cloud service revenues. Source FSB – Third-party dependencies in cloud services – December 2019

[28] Source FSB – Third-party dependencies in cloud services – December 2019.

[29] Resiliency features include: geographical redundancy of data centres, back-ups, cyber-security systems, compliance programmes, automated security controls. Workload mobility features include: containerisation of workloads, open source IT environments…

The outsourcing by financial institutions of core or critical financial activities to CSPs also entails certain micro-level risks that have been identified by the ESAs and are currently being addressed (see Section 3). These include the risk of an inappropriate governance and oversight of cloud arrangements by the customer management[30] or of inadequate due diligence and risk assessments when implementing a cloud contract[31]. Other risks that have been mentioned are: supervisory risks in case supervisors do not have the necessary information to assess the specific risks associated with cloud services or a greater exposure to cyber-security and loss or leak of data risks if cloud outsourcing is inappropriately managed.

Some of these risks may be increased by possible difficulties in the implementation of the shared responsibility model that is used in the context of cloud services, according to some market observers (e.g. if there is an unclear delineation of responsibilities between the CSP and its customers or if customers do not have sufficient expertise or resources[32]). Indeed, while security, risk management and compliance responsibilities are shared between the CSP and the financial institution[33], the latter institution retains the ultimate liability for its own operational resilience and business continuity[34].

3. Existing policy frameworks and initiatives underway in the EU

3.1 Existing EU policy frameworks and codes of conduct concerning outsourcing to CSPs

Generally speaking, the use of cloud computing services is considered at present by financial regulators and supervisors around the world as a form of outsourcing[35]. In the EU, the outsourcing provisions of financial frameworks[36], aiming to ensure a sound governance and risk management of outsourced services apply to cloud services. Information security frameworks (e.g. concerning cyber-security such as the Cybersecurity Act) also apply to cloud services. Data protection frameworks[37] moreover underpin the use and management of personal and non-personal data in the cloud (GDPR, Free flow of data, open data directive…). These frameworks are designed to facilitate data flows and exchanges, including via the cloud, with adequate legal certainty and protection.

Cloud-specific rules have been developed over the last few years in the EU in addition to these generic requirements, focusing on the handling by financial institutions of outsourcing arrangements and the implementation of data portability and reversibility features by CSPs.

Guidance on cloud outsourcing in the financial sector

Cloud outsourcing guidance has been developed since 2017 by the ESAs for the different sectors of finance[38], acknowledging the particularities of cloud services compared to more traditional forms of IT outsourcing[39]. The objective of these guidelines is to help financial firms identify, address and monitor the risks previously mentioned that may arise from cloud outsourcing arrangements at different stages of their implementation and also to foster greater supervisory convergence of cloud outsourcing across the EU.

These 3 sets of guidelines adopt a proportionate approach, focusing mainly on the outsourcing to CSPs of critical or important operational functions[40] and cover similar ground[41], including: the governance, documentation, oversight and

[30] If the management of the financial institution is insufficiently involved in outsourcing decisions, if resources are not appropriate or if financial institutions do not fully grasp the technical implications of using cloud services or the impacts of cloud contracts.

[31] For example that may overlook the specificities of cloud computing or overly rely on CSPs.

[32] There may be complications for some FSIs due to the multiplicity of types of services offered on the cloud (IaaS, PaaS, SaaS…), the constant evolution of underlying technologies, possible additional operational resilience requirements imposed by supervisors on regulated financial institutions. The unbundling of the value chain that cloud solutions entail also raises challenges in terms of supervision, because the full extent of activities performed by the financial institution may be more difficult to grasp.

[33] In the shared responsibility model the CSP is responsible for managing and securing the cloud infrastructure (managing elements such as the provision of servers, networking and data centre facilities and ensuring the security and compliance of the platforms). Customers are responsible for managing aspects such as customer data, application management and user access, adopting security features and configuring services to achieve their resilience targets. Responsibilities are thus shared for activities such as security and compliance including IT controls and risk management. Nevertheless this shared responsibility model does not mean that banks discharge their ultimate accountability on CSPs, as the ultimate liability for any activity will always be held by the bank. (Source AFME – The adoption of public cloud computing in capital markets – November 2019).

[34] e.g. the responsibility for adopting security features and for configuring services to achieve the resilience targets defined

[35] Some outsourcing guidelines dedicated to cloud services have been provided at the global level by the BCBS for the banking sector, but there are no global rules specifically concerning cloud services for capital markets or insurance.Source FSI insight – Regulating and supervising the clouds – December 2018.

[36] Banking and insurance prudential frameworks (Solvency II, CRD) and capital market regulations (MiFID II, CSDR)

[37] EU data frameworks include the GDPR regulation concerning personal data (General Data Protection Regulation) that ensures that individuals remain in full control of their data; the Regulation on the free flow of non-personal data across the EU; and the Open Data directive (concerning the re-use of public sector information) - to which sector-specific legislation on data access has been added, such as the Payment Services Directive (PSD 2).

[38] A first set of guidelines was published by the EBA for the banking sector in 2017 and revised in 2019. This revision entered into force at the end of 2019 and is being implemented by the NCAs. Following the recommendations made in the Fintech action plan (March 2018) guidelines were also published by EIOPA in February 2020 for the insurance sector and guidance has been proposed by ESMA for capital market participants in June 2020.

[39] Notably the fact that cloud services are more standardised than usual ICT services and provided to clients on a large scale and in a highly automated manner.

[40] A definition of "critical or important operational functions" is given in MiFID II. An operational function is considered as critical or important where a defect or failure in its performance would materially impair the continuing compliance of a financial firm with the conditions and obligations of its authorisation and its obligations under EU regulations, its financial performance or the soundness and continuity of its services and activities.

[41] This seems logical since the main risks associated with cloud outsourcing are similar across sectors.

monitoring mechanisms that firms should put in place; the assessment and due diligence, which should be undertaken prior to outsourcing; the minimum elements that outsourcing and sub-outsourcing agreements should include; the exit strategies and the access and audit rights that should be catered for; the notification to the competent authorities and the supervision carried out by them[42].

Data portability and reversibility self-regulatory codes of conduct

Self-regulatory codes of conduct complete these guidelines.

In the context of the Digital Single Market (DSM) initiative, the SWIPO stakeholder group (switching and porting) has drafted two self-regulatory codes of conduct regarding the porting of data across different cloud infrastructures: one concerning IaaS portability and the other SaaS portability. The objective is to reduce the risk of vendor lock-in by CSPs and make the European markets for cloud services more fluid and competitive. The implementation of these codes was initially planned for May 2020.

The CISPE trade association (Cloud Infrastructure Service Providers in Europe) has also been working together with the European association of CIOs (EuroCIO) on a reversibility code for cloud infrastructure services in order to facilitate provider changes.

GDPR codes of conduct

Self-regulatory codes of conduct have been developed in connection with GDPR. For example, an EU Data Protection Code of Conduct for CSPs has been developed by the EU Cloud Code of Conduct General Assembly. The Cloud Security Alliance Code of Conduct for GDPR Compliance is moreover designed to offer both a compliance tool for GDPR compliance and transparency guidelines regarding the level of data protection offered by CSPs[43].

3.2. Additional initiatives underway in the EU

Additional proposals have been made by the Commission and the ESAs in order to address the challenges associated with an increasing use of cloud service outsourcing in the financial sector. These focus on defining common rules and supervision mechanisms for CSPs. The objective to foster the development of a cloud ecosystem respecting EU rules has also been put forward by the Commission.

EU cloud services rulebook and marketplaces

The development by Q2 2022 of a European cloud rulebook building on existing codes of conduct and certifications was proposed by the Commission in the Communication on a "European strategy for data" (February 2020), which aims to create a single market for data in the EU hinging on common interoperable data spaces in different strategic sectors, including finance[44].

A further proposal of the Commission is the setting up of a cloud services marketplace for EU public and private sector users, offering cloud processing software and platform services complying with requirements of the EU cloud rulebook in areas such as data protection, security, portability, energy efficiency, etc. Participation in the marketplace for CSPs would be made conditional on the use of transparent and fair contractual conditions. The signature of Memoranda of Understanding with Member States on cloud federations in Q3 2020 would be a first step of this initiative, in order to avoid a multiplication of fragmented cloud federations and data-sharing initiatives across the EU.

GAIA-X, a European cloud federation backed by Germany and France and involving a number of CSPs, software and ICT service providers, was launched at the end of 2019, in line with these proposals. The objective is to develop a cloud infrastructure and data ecosystem in the EU[45] based on European values and common goals including: data sovereignty[46], data availability, interoperability, portability, transparency and fair participation. Functioning as a non-profit organisation, the GAIA-X structure will ensure the governance of the initiative and the application by the participating firms of the requirements mentioned above. GAIA-X will certify in particular that information remains secure and provide guarantees about where it is stored and how it is processed. Moreover common portability and reversibility standards will allow customers to move their data and workloads from one GAIA-X provider to another.

Oversight of critical third-party service providers

Following proposals made by the Joint Committee of the ESAs regarding ICT risk management requirements[47], the Commission

---

[42] ESMA consultation paper on Draft Guidelines on Outsourcing to Cloud Service Providers – June 2020 https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf; EBA revised Guidelines on outsourcing arrangements https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.

[43] See https://eucoc.cloud/en/home.html#:~:text=In%20this%20context%2C%20the%20EU,cloud%20services%2C%20based%20on%20GDPR and https://cloudsecurityalliance.org/artifacts/cloud-security-alliance-code-of-conduct-for-gdpr-compliance/#:~:text=The%20CSA%20Code%20of%20Conduct,by%20the%20Cloud%20Service%20Provider.&text=Help%20CSA%20better%20understand%20how%20we%20can%20support%20the%20cloud%20community.

[44] The Commission's objective with this proposal is to establish common interoperable data spaces in strategic sectors at EU level by combining investments in next-generation data infrastructures, the interconnection of existing cloud and edge infrastructures and computing capacities and related tools and governance mechanisms. The Commission also put forward in this Communication, rules for facilitating the access to data and its use and sharing and also the enhancement of data rights across the EU, which should also contribute to tackling some barriers impeding the development of cloud services in the EU.

[45] The GAIA-X ecosystem comprises a data ecosystem fostering the development of EU data spaces, an infrastructure ecosystem using common standards and also federation services i.e. a set of common services used by federation members concerning identity and trust, data exchange, compliance etc.

[46] Data sovereignty is defined in this instance as a complete control over stored and processed data, also including the independent decision on who is permitted to have access to it.

[47] https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

is currently considering the possibility of establishing a form of oversight of third-party ICT providers that are critical for financial institutions, including CSPs[48]. The objective is to better address the risks posed by a more widespread use of outsourced services, including cloud, and related concentration risks and also to ensure a consistent supervision of critical third-party providers across the EU.

This future proposal is part of the consultation undertaken during Q1 2020 by the Commission on a possible digital resilience framework for financial services, which is a component of a wider effort to implement a new digital finance strategy for the EU. The envisaged framework would set out criteria for identifying the critical nature of third-party ICT providers, define the extent of the activities that are subject to the framework, establish consistent oversight tools and mechanisms and designate the authority responsible for carrying out the oversight.

Standard contractual clauses

Following a recommendation made in the Fintech action plan (March 2018), the Commission is working together with stakeholders, supervisors and regulators on the definition of standard contractual clauses for outsourcing agreements between financial institutions and CSPs[49]. The objective is to raise legal certainty regarding cloud use in the financial sector. The EU-wide application of the standard contractual clauses should also help to improve supervisory convergence. An initiative has also been conducted previously to develop guidelines for standardised Cloud Service Level Agreements (Cloud SLAs). Other initiatives are also underway in these areas in certain Member States.

European cybersecurity cloud certification scheme

The Commission requested ENISA, the EU agency for cybersecurity, at the end of 2019 to prepare a cybersecurity certification scheme for the cloud in the context of the European Cybersecurity Act in order to demonstrate the equivalence of security requirements throughout Europe, overcome the present patchwork of cloud security certification schemes and facilitate the cross-border storing and processing of data, while also facilitating the comparison of CSPs with respect to security when switching providers.

Written by Marc Truchet, Eurofi

[48] The expert group mandated by the Commission to identify regulatory obstacles to financial innovation (ROFIEG) also proposed in December 2019 the introduction of more binding frameworks for third-parties in the form of certification and licencing regimes, beyond the revision of existing governance and outsourcing requirements. The objective of this proposal is to enhance cross-sectoral risk management and also allow for more effective oversight of outsourced services in a context where financial firms are increasingly dependent for critical services on third-parties that operate in a concentrated market with high market power.

[49] This objective has also been put forward by the High Level Forum on the CMU in June 2020 for cloud services in the capital market area, together with rules to ensure the secure use of cloud services notably with specific cyber-resilience measures

ANNEXE

Main benefits and risks of cloud services and barriers to their implementation

Potential benefits

Flexibility and innovation: Cloud services contribute to lowering barriers to entry and facilitate innovation and growth both for fintechs and incumbents. Cloud services indeed allow the development, testing and scaling up of new services without supporting high upfront investments in IT and help to accelerate the time-to-market for the launch, evolution or geographic expansion of new digital and data-driven services[50]. Cloud services can also improve flexibility, allowing business models to adapt and processing capacities to adjust to changes in demand e.g. a seasonal peak of activity.

Cost efficiency: The use of cloud services reduces the initial capital expenditure investment required for traditional on-premise IT infrastructure and IT administration costs and can also help to optimise costs by better adjusting computing capacity to what is needed to serve customer demand[51]. Cloud also reduces the need for redundant capacity and back-up mechanisms that are usually needed with traditional IT architectures.

Risk mitigation: Security concerns were a major barrier to the adoption of cloud services in the past. However recent assessments show that the security capabilities of CSPs and their capacity to mitigate operational risks are not lower than those of on-premise IT and may actually be higher than those that most individual financial institutions can put in place in-house[52]. Indeed all the users of cloud services benefit from the security features implemented by CSPs on their platforms, which are constantly updated (e.g. redundant data centres, back-ups, cyber-security systems, compliance programmes, automated security controls…) and their expertise in this area.

Main barriers to cloud adoption

Legacy IT infrastructures: The existence of legacy IT architectures owned by financial institutions is a first barrier. Adopting cloud services requires switching to a pay-per-use model and progressively downsizing existing infrastructure. This may take time, meaning that for some firms cost savings are mainly in the form of future cost avoidance rather than short term reductions. Legacy IT systems are also often interconnected making the transition of certain processes or activities complex. Adopting cloud services at scale may also require adjusting certain core financial or business processes (for example transaction execution and settlement processes) in order to effectively embed interactions with cloud service platforms.

Skills and cultural barriers: The implementation of cloud services usually entails changes in IT roles and responsibilities that require training and coaching the existing workforce and possibly bringing in new cloud-specific expertise. For example functions such as database administration, network or storage management may not be required to the same extent and more resources may be needed to manage relations with third-party CSPs. There are also cultural and trust barriers to also take into account when moving to the cloud as decision-makers and managers need to be convinced of the safety and benefits of these new solutions.

Fragmented regulatory landscape: The fragmented regulatory landscape in the EU regarding cloud services is a challenge, that is however progressively being alleviated with the implementation of the guidelines published by the ESAs (see detail in Section 3). The risk of different interpretations between the NCAs of these guidelines or of certain criteria impacting the way they are applied however subsists, since they are not underpinned by a European regulation.

Legal issues related to data: While EU level rules applying to data such as the GDPR define common requirements, variations remain at the Member State level in the way some data rules are interpreted and also in data location or local "mirroring" rules[53] aiming to protect domestic interests. This adds complexity to the adoption of public cloud at scale across the EU and makes it more difficult to leverage global risk management and compliance programmes proposed by CSPs[54]. In addition, the cross-border nature of CSPs exposes them to potential legal requirements imposed by their home country, such as the US Cloud Act[55] which may create confusion or be perceived as a threat to EU customers. Personal data privacy is however protected by GDPR in the EU which reduces these issues in the area of retail financial services.

Potential risks

Potential financial stability risks: Potential financial stability risks due to the third-party dependencies created by cloud services and the concentration of the CSP market were emphasized by the FSB[56]. As with any outsourcing, cloud service users are exposed to the operational risks faced by CSPs that may lead to business continuity issues. However, the high concentration of the current cloud services market and the increasing scope of activities and processes delegated to CSPs, may increase these risks. If one or several major CSPs are severely disrupted, this may not only create business continuity risks but also potential financial stability risks for the whole market. These challenges may be amplified by vendor lock-in limitations (e.g. due to specific contractual terms) or workload or data portability issues (e.g. due to differing technical features).

---

[50] This however requires changes in the way projects are conducted e.g. adopting a "devops" approach for developing and deploying applications as a set of smaller processes and adapting duties within the development team.

[51] for example during peak (or low) periods of activity or across different jurisdictions.

[52] See for example the Garner report "Is the cloud secure?" March 2018 Report. On average the security failures and incidents experienced by CSPs are lower than for traditional infrastructures. The FSB report on Third-party dependencies in cloud services mentions that from a technological perspective large public CSPs can often offer an IT environment that is at least as robust as the one individual financial institutions could create on their own premises.

[53] For example the location rules imposed by the German Data Protection Authority that impose "safe harbour" requirements when using a non-EU based CSP.

[54] Source AFME report on The adoption of public cloud computing in capital markets (Nov 2019) and FSB report on Third-party dependencies in cloud services – December 2019.

[55] The US Cloud Act adopted in 2018 provides US government agencies with rights of access to public cloud data managed by US CSPs.

[56] Source FSB – Third-party dependencies in cloud services – December 2019.

The multi-cloud and hybrid strategies increasingly adopted by financial institutions and containerisation and open source approaches put in place by CSPs contribute to mitigating these risks, even though portability is not ensured by binding rules.

Definition and implementation of shared responsibilities: Some of these risks may be amplified by an unclear delineation of responsibilities between financial institutions and CSPs. Indeed with the shared responsibility model[57] used in the context of cloud services, the ultimate liability for its own operational resilience and business continuity is held by the financial institution[58], although security and compliance responsibilities for example are shared between the CSP and the financial institution. The specific issues faced by smaller financial institutions who may not have sufficient bargaining power vs large CSPs to impose e.g. audit rights or to conduct appropriate risk assessments has also been raised.

Micro-level risks: A number of other more micro-level risks that financial institutions may face when implementing and operating cloud outsourcing arrangements were moreover identified by the European Supervisory Authorities (ESAs)[59]. These include the risk of an inappropriate governance and oversight of cloud outsourcing (if the management of the financial institution is insufficiently involved in decisions or if resources are not appropriate); inadequate due diligence and risk assessments that may overlook the specificities of cloud computing or overly rely on CSPs; cyber-security and loss or leak of data; supervisory risks in case supervisors do not have the necessary information to assess risks.

Written by Jean-Marie Andrés , Eurofi

[57] In the shared responsibility model the CSP 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. Responsibilities are shared for activities such as security and compliance including IT controls and risk management. Nevertheless this shared responsibility model does not mean that banks discharge their ultimate accountability on CSPs, as the ultimate liability for any activity will always be held by the bank. (Source AFME – The adoption of public cloud computing in capital markets – November 2019).

[58] This may be further complicated by the multiplicity of types of services offered on the cloud (IaaS, PaaS, SaaS…), the constant evolution of underlying technologies and possible additional operational resilience requirements imposed by supervisors on regulated financial institutions. The unbundling of the value chain that cloud solutions entail also raises challenges in terms of supervision, because the full extent of activities performed by the financial institution may be more difficult to grasp.

[59] ESMA consultation paper on Draft Guidelines on Outsourcing to Cloud Service Providers – June 2020 https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf.