EU FINANCIAL DATA SPACE AND CLOUD INFRASTRUCTURE

1. Opportunities and challenges associated with the development of cloud services in the financial sector

1.1 Current trends of cloud service use in the financial sector

An industry representative explained that there is momentum for cloud services adoption in Europe, particularly in the financial services industry. Cloud has generally evolved as one of the key enablers of digital transformation. Digital native and challenger banks were early adopters of cloud and are now followed by more traditional financial players.

There are several trends underway in the financial industry concerning cloud services. One is the ongoing transformation of the core IT infrastructure of financial institutions, with a movement away from legacy systems and a progressive adoption of cloud-based systems, which are proving to be more agile and often more secure and resilient. Second, moving to the cloud can help traditional players to facilitate and speed up innovation regarding their key processes. Third, cloud services can also support regulatory processes, allowing supervisors and regulators to receive more up-to-date information in a more structured and automated manner. Finally, there is a great deal of innovation happening in the know your customer (KYC) and anti-money laundering (AML) fields thanks to the cloud, where the industry is deploying artificial intelligence (AI) and machine learning solutions to move away from rules-based systems and address AML issues with a more risk-based approach.

The Chair noted that the speed of change is remarkable in this area. Until recently, the focus was mainly on cloud adoption and transitioning customers to the cloud. But now the cloud appears to have become a major driver of transformation at the heart of many key financial processes such as risk management and reporting, which also calls for greater attention from supervisors than before.

1.2 Main opportunities offered by the use of cloud services

A policy-maker stressed that cloud computing can boost the cost, efficiency and agility of data processing, and therefore make European businesses more competitive. It can also facilitate data sharing across different business actors of the same ecosystem and can foster the emergence of an innovative data system in different sectors. Cloud is therefore at the heart of the open banking evolution due to its potential for supporting commercial relationships between different types of financial institutions, including fintechs, which have often been operating in the cloud from the very beginning.

The cloud can also unlock access to a number of emerging technologies, such as AI and blockchain, thus helping to trigger a second wave of digital transformation in the financial sector and allowing the financial sector to remain at the forefront of this transformation. Operating on a pay-per-use basis, cloud can make these technologies easily accessible and scaleable, without having to use a traditional IT infrastructure. This can lead to major savings in terms of capital expenditure. A Commission study found that the average organisation can reduce its IT infrastructure cost by 30-50% when moving to the cloud. Cloud also facilitates access to important added-value services. Financial institutions are, for instance, running on the cloud AI systems for robo-advice, credit scoring applications and chatbots that engage with consumers. There can also be cloud-native running of DLT for digital currencies or DNS resolvers on the cloud that preserve privacy and help to reach a high level of security.

Finally cloud computing can help to address problems of interoperability between legacy IT systems and new systems which are multiplying with the speed of evolution of technologies. These problems often happen in large financial institutions where multiple pieces of software and multiple databases in silos co-exist. Cloud computing has the potential to change this paradigm by providing fully interoperable and, ideally, vendor-neutral solutions.

An industry representative stated that it is very important to consider the practical use cases of cloud in the policy discussion. Using cloud services enables a real reduction of IT costs. This is mainly true when using public cloud service providers (CSPs) and hyperscalers, because whilst setting up a private cloud might be a first step it will not provide the same benefits. Secondly, buying services out of the public cloud for data analytics or AI offers access to higher processing capacities, which allow for example the evaluation of more complex financial instruments requiring many calculations. Finally, another advantage of the cloud is its flexibility. With the pay-per-use model, computation power can be bought when it is needed and there can be a progressive revamping of applications and IT systems on the cloud. With this 'continuous development' financial institutions are able to provide clients with innovations on a more frequent basis.

A regulator explained that the supervision of companies with activities in the cloud has revealed several opportunities. On the industry side, these include a greater capacity to innovate and enhance products and customer experience with greater convenience. The use of cloud services can also increase competition, flexibility and choice in the financial sector, and can help financial institutions to transition from their legacy systems. Cloud services can also support regulatory and supervisory activities by facilitating access to supervisory and regulatory technology (SupTech and RegTech). These are innovative technologies that can be embarked on underlying cloud infrastructures and can ensure the continuity of regulatory and supervisory activities with the financial entities concerned.

1.3 Conditions and challenges associated with the development of cloud services

A policy-maker suggested that different factors of success need considering when moving to the cloud. First, financial institutions should be encouraged to adopt a multi-cloud strategy with a balance across multiple cloud providers in order to avoid putting all their eggs in the same basket. Second, proper attention should be paid when negotiating cloud contracts. There are many potential problems of asymmetry in negotiating power with CSPs and even fairly large financial institutions find it challenging to negotiate cloud contracts in some cases. That is why the European Commission is currently developing standard contractual clauses for cloud use by financial institutions. Another factor of success is to establish a cloud centre of excellence in the organisation. Organisations should adopt a central IT risk strategy with a multi-cloud element, as also mandated by the new Digital Operational Resilience Act (DORA) legislative proposal.

An industry representative noted that the broader uptake of cloud services raises several challenges for the financial sector. There is a skills challenge, because moving to the cloud is a relatively new journey which comes with many change management aspects. Although this issue is probably less acute in finance than in other sectors, the industry is still defining the optimal path for moving to the cloud in a safe way. There are also potential concerns related to concentration risk and vendor lock-in, which regulators are working to address. From an industry perspective, open-source technology and multi-cloud approaches that foster portability and interoperability are ways to address this problem and to insure financial institutions against the possible failure of the systems of one given provider. A third challenge is regulatory fragmentation. Whilst a very significant effort has been made by the European supervisory authorities (ESAs) in the past few years to define a harmonised approach to outsourcing rules, there is still fragmentation at the member state level in their implementation and supervision. It is hoped that further policy efforts, including with DORA, will help to alleviate these problems.

A regulator added that while the technological sophistication brought by cloud services delivers clear benefits to financial services firms and their customers, it also changes the nature of the operational risks that need to be managed and mitigated by financial institutions and may create new complexities e.g. in terms of data localisation. Concerning the further source of complexity brought by the variations that exist across regulatory requirements, the regulator confirmed that.it is one of the objectives of DORA to address this issue and create more convergence at the regulatory level.

A public representative observed that a further challenge that is not specific to cloud is that technological innovation is often faster than regulation. However, the EU institutions are conscious of this and are trying to improve the way regulations and frameworks are updated.

1.4 Main opportunities and challenges associated with enhanced data use and sharing

An industry representative stated that data access, data sharing and the cloud are the basis of a potential revolution in the insurance industry in particular. Insurance companies aim to move away from being perceived as just traditional claims-driven companies and reimbursement agents to becoming 'lifetime partners' of customers, providing a range of assistance and prevention services. This may be supported by the combination of insurance and technology, and in particular the Internet of Things which allows access to continuous flows of data that come on a real-time basis. Historically the industry has been based on single data points, especially for underwriting purposes, but this is now evolving. With continuous flows of data from customers, timely assistance and prevention can be effectively provided, above and beyond paying claims.

There are a number of challenges however that the insurance industry is facing in this context of increasing digitalisation. First is the risk of inertia that is common to large incumbent multinational companies facing legacy systems and localised regulations that constitute barriers to change. Another challenge is providing sufficient value to customers for sharing their data and also safeguarding the use of data when it is processed in the context of AI or aggregated with other data sources. A further challenge is the competition brought by big technology firms and new entrants that do not have the same legacy systems and operating models and which requires a level playing field to be established.

2. Priorities for the regulation and supervision of cloud services and data use and sharing

In the second part of the discussion, the panellists commented on the main regulatory initiatives underway related to cloud services and the use and sharing of data.

2.1 Digital Operational Resilience Act (DORA) and the ESA cloud outsourcing guidelines

A policy-maker stated that having an appropriate regulatory architecture for cloud services is important for ensuring legal certainty and is beneficial for both the financial services industry and cloud service providers (CSPs). The objective of DORA is to address the threats to operational resilience in the financial sector associated with the use of new technologies including cloud, by further harmonising and streamlining existing rules on ICT[1] risk management and ICT-related incident reporting. The risk-based approach taken in DORA is directly inspired by the Network and Information Security (NIS2) directive, which provides legal measures for improving cyber-security in the EU, but DORA looks at the specific requirements of the financial sector. DORA aims at addressing different issues mentioned in the context of cloud agreements - such as the risk of vendor lock-in, the imbalances in contractual negotiation, the exit strategy when a bank or financial institution wants to switch providers, or concentration risk - by introducing a certain number of high-level requirements for contractual agreements between

1. ICT: Information and Communications Technology

financial institutions and third-party IT providers. It also introduces oversight by the ESAs over critical CSPs.

In terms of implementation, DORA will be supplemented by Level 2 and Level 3 guidance at a European level. Level 2 will be materialised by the existing cloud outsourcing guidelines published by the ESAs in 2019 and 2020 that provide an appropriate basis for the implementation of DORA. The proposal is to also put in place Level 3 rules by developing standard contractual clauses for cloud outsourcing specifically for the financial sector, based on the Level 1 DORA guidelines and the outsourcing guidelines of the ESAs. It is believed that this more harmonised framework at the EU level will help to speed up the time to market for cloud projects in the financial sector and support innovation. This three-level architecture should also facilitate supervisory convergence for cloud outsourcing across the EU.

A regulator emphasized that the ESA cloud outsourcing guidelines were a pioneering work that gave the initial structure and perspective on how cloud service provision should be structured and on the issues that should be taken into consideration for its proper oversight in the financial sector. While there are three different guidelines from the ESAs, these enjoy a high level of convergence. For instance, all three guidelines mention general principles of governance, define requirements for an appropriate outsourcing policy (e.g. in terms of documentation, allocation of responsibilities) and describe how the outsourcing process should be carried out from the pre-outsourcing phase to the exit strategy. The guidelines also define risk management and due diligence requirements and the determination of whether a CSP is of critical importance for a financial entity. This therefore provides financial institutions with an appropriate basis for negotiating and structuring their cloud contracts and supervisors with guidelines for conducting the oversight of cloud-related risks. The DORA proposal builds on these guidelines to a large extent and has many aspects in common.

An industry representative stated that cloud is essential for the competitiveness of the financial sector and should be thought about not just from a risk standpoint but also from the standpoint of what is required to enable its effective implementation in Europe. Indeed the major CSPs invest a great deal in securing their operations, which may contribute to actually reducing operational risks in the financial system. In this regard DORA is a step forward because it provides a common framework and will help to reduce the current fragmentation of rules. It is necessary however to make sure that the specific risks associated with cloud (compared to the outsourcing to a data centre) are understood. The current proposals are also very focused on applying outsourcing rules to cloud services and could potentially be extended to any ICT services sold on a pay-per-use basis and which can be bought and terminated quickly.

A public representative emphasized that concerning cyber-security there are a number of intersections between DORA and NIS2. This is normal because DORA builds on NIS2 but the connection between the two legislations needs to be more clearly established. Further work and coordination is needed on a number of issues: for example according to the NIS 2 proposal, CSPs should be from now on classified as 'essential entities' and should thus be subject to both the requirements of DORA and NIS 2, but there is no clear hierarchy between DORA and NIS 2 requirements in that regard. This brings a clear issue of taxonomy in incident reporting and potential overlaps in the requirements for CSPs. The question is whether this redundancy is intentional because the regulator sees the need for increased oversight of CSPs or if it is unnecessary duplication. There is also an issue regarding the coordination between the lead overseer introduced in DORA and the national competent authorities (NCAs) defined in the NIS2 Directive. Strong coordination is needed between the EU and Member State level, otherwise that will lead to fragmentation.

An industry representative stated that DORA is a novel framework. Indeed, it is for the first time bringing ICT providers into the scope of financial services oversight and this must be done appropriately. DORA could create a genuine opportunity to enhance understanding, transparency and trust between ICT service providers, financial entities and regulators and ultimately stimulate innovation in the European financial sector. However, to ensure its effectiveness a certain number of issues need to be considered. The consistency of DORA with the NIS Directive is critical, the industry speaker stressed. DORA is not lex specialis for providers who may be subjected to other parallel frameworks and might end up being confronted with two packages that have conflicting recommendations, issued from different authorities that have not sufficiently coordinated. In this perspective there is a need for legislation to harmonise and deduplicate requirements, including between DORA and existing frameworks like the ESA Outsourcing Guidelines and the NIS Directive - in particular in the view of the new NISD2 proposal. Legislation must also be proportionate and fit-for-purpose, especially through the requirements that recognize the technological realities of evolving ICT services in the public cloud context - that are provided in a multitenant, one-to-many environment. There is a need to maintain technology neutrality and boost innovation, which is encouraged by open markets and the free flow of data, and also to protect the availability and integrity of digital services and cloud customers' privacy, whether they are subject to DORA or not. It is to be hoped that these issues will be addressed in the on-going legislative process.

2.2 Data Services Act (DSA)

A public representative noted that the DSA proposed in December 2020 could be of importance for data-related issues. The actual work is still on hold because some internal decisions are being waited for. This regulation builds on the principle of the e-Commerce Directive. It is going to touch upon the liability exemption and the general monitoring prohibition. In that matter, the regulation can be divided into two main aspects. The first one is guaranteeing data safety for customers and safety online in general. A second is how to regulate the industry and the main providers.

An interesting new insight, the public representative believed, is that it will be ensured that there is a proportional obligation depending on the size of the provider and the number of users the provider is serving. The objective with the DSA is to ensure by regulation that the fundamental rights of the users are

safeguarded. Usually this objective is in the hands of the providers and requires a great deal of effort with the pre-existing directives and frameworks. This remains a priority for the European Parliament, especially in the current environment where the exposure of online users in education and working spaces has increased in the last few months.

An industry representative noted that, generally speaking, with the pace of change that all observe in technological developments, the continued review of existing regulations and policies is essential. It has to be ensured they are up to the standards of the current technological developments and foresee any changes in the future. This is, for example, very applicable to GDPR, which is a great regulation that has set the standard on a global basis. Nevertheless, there should also be consideration of how other regulatory environments diverge from the EU, and from GDPR specifically, because this divergence may limit access to some potential developments that could be better exploited at a European level if GDPR was reviewed.

An industry representative added that for the data privacy and security issues there will be more practices going forward. There have been some discussions about whether someone putting their name on a video platform already presents a data privacy issue for example. Those kinds of things have to be settled, otherwise the application of these requirements becomes very difficult for the industry.

Conclusion

The Chair summarised that cloud services and data access and sharing are at the heart of the transformation of the banking and insurance sectors. Use cases show that cloud services are entering more into the core tasks and processes of financial institutions. On the one hand, this offers new opportunities to improve services and better serve customers. On the other hand, this implies important changes to business and operating models, which may raise new risks and financial stability issues. However, cloud outsourcing and other innovative technologies may also contribute to mitigating stability risks in the financial sector.

Everybody on the panel agreed that the initiatives of the Commission, in particular the DORA initiative are moving in the right direction. However some technical issues and potential inconsistencies between DORA, NIS 2 and the ESA cloud outsourcing guidelines need to be addressed for enabling the European financial industry to reap the full benefits of data, digital innovation and the cloud.