Cloud computing is a technology enabler. It allows cost reduction, flexibility, scalability and a better use of IT. However, it is only being gradually adopted by banks. There is no regulatory harmonisation, neither globally nor at EU level, and there is a need to bring agility to cloud adoption by financial institutions.

Cloud is typically delivered in the form of IaaS (infrastructure as a service), PaaS (platform as a service) or SaaS (software as a service), through public, private or hybrid clouds. This technology is gradually being adopted by financial institutions (FIs), although its use is not yet widespread, as most FIs still rely on in-house infrastructure or use cloud services only for the non-core part of the business. In its Digital Single Market Strategy, the European Commission (EC) considers cloud as an economic game changer, recently publishing a Cloud Computing Initiative. As regards the Financial Stability Board (FSB), it has published several documents with an explicit reference to outsourcing as an important element to take into account for an effective risk appetite framework or referring to operational continuity as a going concern supervisory consideration, also present in the context of outsourcing.

From the National Financial Supervisory Authorities (NFSAs) standpoint, cloud is considered a form of outsourcing and therefore the same rules apply. NFSAs perform evaluations and cloud adoption is subject to requirements that prevent FIs from streamlining cloud workloads. Despite the fact that many NFSAs in Europe (Spain, Netherlands, Greece, Finland, among others) have published opinions on this matter, with both recommendations and obligations related to outsourcing or cloud based services, the financial industry is dealing with a lack of clear and formal guidance that is consistent across all NFSAs. As for the most recent guidance on outsourcing published by financial authorities, the FCA in the UK and the MAS in Singapore (July 2016) stand out. There is a need for harmonisation across EU financial supervisory regulation and a need to speed up and bring more agility to the cloud adoption process in order to improve cost efficiency and scalability, as essential elements for a digital transformation of the financial sector.

Moreover, there is a need for a better understanding of cloud technology by the supervisory authorities, particularly in relation to security and risks. NFSAs are assessing the implications of migrating workflows to the cloud before allowing a wide adoption of these technologies. Security and privacy are considered two of the main reasons preventing a wider adoption of Cloud, according to the European Union Agency for Network and Information Security (ENISA).

Compliance with Data Protection Law

Financial institutions need to comply with data protection regulations. A cloud computing contract with a cloud service provider (CSP) usually implies an international data transfer, where typically the bank acts as a

data controller and the CSP as a data processor\(^6\). For this reason, compliance with Directive EC/95/46 on Data Protection (which will be replaced by the General Data Protection Regulation 2016/679 from 2018) must be ensured, particularly as regards the general need of approval by the National Data Protection Authorities (NDPAs) when transferring data outside the European Economic Area (the EU, Iceland, Liechtenstein and Norway) and compliance with articles related to international data transfers. Moreover, some NDPAs have also published guidance for Data Protection compliance in the cloud computing context, as it is the case of the Spanish authority, which published guidelines (2013) targeted at both cloud computing users and CSPs\(^7\). As for the European Commission, it is currently working on a Data Protection Code of Conduct for CSPs\(^8\).

**Managing Cyber Security**
Governance, security and privacy are still considered key challenges. In relation to information security measures, these are dispersed across many European and national legislations. There is a large body of related work on the security and governance aspects of cloud computing, including the work by ENISA. Some of the main obstacles constraining a mature cloud adoption are the lack of harmonised internationally recognised standards, certification, data protection issues and interoperability (difficulties when switching providers and lock-in effects).

![Cloud Computing Challenges](image)

**Figure 1.1**

**Conclusion**
EU institutions in cooperation with NFSAs should continue their work to harmonise the legal and regulatory environment within the EU. It is clear that a better understanding by NFSAs of information security and cyber security risks related to the adoption of cloud computing would greatly help the market mature and improve. Gaining agility and, thus, reducing time-to-market in migrating workloads to the cloud by financial institutions is essential. From a data protection perspective, European NDPAs should follow the same criteria when approving processors from outside the EEA. Since the cloud is a global and cross-border technology, there is a need to set common grounds and a baseline for cloud computing regulation across the globe with a risk-based approach. Nowadays, the end user is thinking and acting globally, demanding banks to also act in a global manner and regulators and supervisors should also be aware of this challenge.

---

6: According to Art.4 of the GDPR 2016/679, a data controller means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...[...]”. A data processor means “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.


DISCLAIMER
This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.
Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.
This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes. BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.
This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.
In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.
The content of this document is protected by intellectual property laws. It is forbidden its reproduction, transformation, distribution, public communication, making available, extraction, reuse, forwarding or use of any nature by any means or process, except in cases where it is legally permitted or expressly authorized by BBVA.