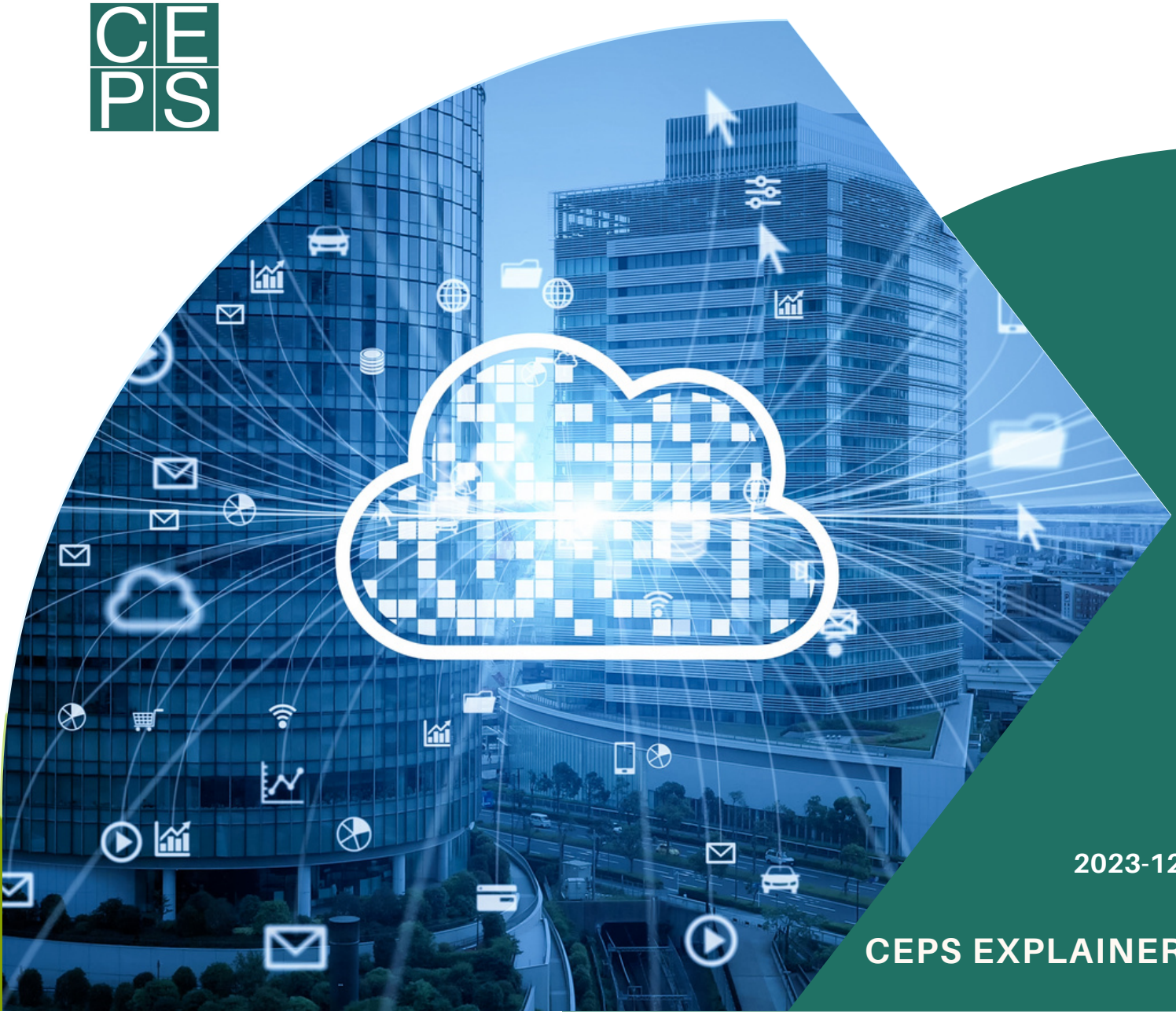


2023-12

CEPS EXPLAINER

THE BANKING SECTOR IS INCREASINGLY LOOKING TO THE CLOUD

But what are the real risks and opportunities for a new regulatory framework?

Judith Arnal

SUMMARY

Digital transformation is an unstoppable process that has substantially accelerated since the Covid-19 pandemic. As one of the targets of the Digital Decade, at least 75 % of EU companies are expected to use the cloud, Big Data or AI technology by 2030.

The banking sector has not remained on the sidelines of cloud technology's growing relevance. Although the Financial Stability Board concluded in a 2019 report that cloud computing doesn't pose an immediate risk to financial stability, a few years have since gone by and the use of the cloud by the industry is growing.

This has prompted a supervisory and regulatory response that, in the EU's case, has translated into the adoption of the Digital Operational Resilience Act (DORA). Though DORA entered into force on 16 January 2023, it will only apply from 17 January 2025. Still, at present, there is no legal vacuum and in the case of the banking sector, the European Banking Authority's Guidelines on Outsourcing Arrangements are indeed applicable.

Yet a number of myths have been circulating when it comes to the supervisory practices of cloud services usage by the banking sector and this CEPS Explainer refutes them. Besides, though the risk types of an on-premise or cloud model are essentially the same, it is risk governance that differs. Moreover, there are means to mitigate the two most relevant risks (concentration and vendor lock-in risks).

Finally, cloud is an opportunity for banks to really focus on their core business, which is a key reason to avoid any unwarranted protectionist measures.

Judith Arnal is a CEPS Associate Senior Research Fellow in the FMI Unit. The author would like to acknowledge the Master in Banking and Financial Regulation of University of Navarra for helpful and productive seminars on cloud computing in the banking sector.

CEPS Explainers offer shorter, more bite-sized analyses of a wide range of key policy questions facing Europe. Unless otherwise indicated, the views expressed are attributable only to the author in a personal capacity and not to any institution with which he is associated.

The relevance of cloud technology, its benefits and risks

Digital transformation is an unstoppable process that has substantially accelerated since the start of the Covid-19 pandemic and is now spreading across all economic sectors. If our economy is to remain competitive, the EU needs to make decisive progress on the so-called digital transition (twinned with the also ongoing green transition). On the digital front, efforts at EU level are guided by the Digital Decade policy programme, which – amongst others – has set the target of at least 75 % of EU companies using cloud, Big Data or AI technology by 2030.

ON THE DIGITAL FRONT, EFFORTS AT EU LEVEL ARE GUIDED BY THE DIGITAL DECADE POLICY PROGRAMME, WHICH – AMONGST OTHERS – HAS SET THE TARGET OF AT LEAST 75 % OF EU COMPANIES USING CLOUD, BIG DATA OR AI TECHNOLOGY BY 2030.

Cloud computing presents a number of advantages. First, *scalability and flexibility*. Thanks to the cloud, companies can easily scale their resources up or down as needed, without having to invest in additional hardware or software, thus responding quickly to changes in demand.

Second, *cost savings*. Unlike traditional models that require heavy up-front investments in hardware and software, the cloud operates on a subscription model that also allows for payments to reflect actual usage.

Third, *security and compliance*. Cloud computing providers invest heavily in security and compliance measures to protect their customers' data. They use advanced encryption, access controls and monitoring tools to ensure data confidentiality, integrity and availability.

And finally, *innovation*. By leveraging cloud services and tools, companies can create new applications, experiment with new technologies and collaborate on projects in real time.

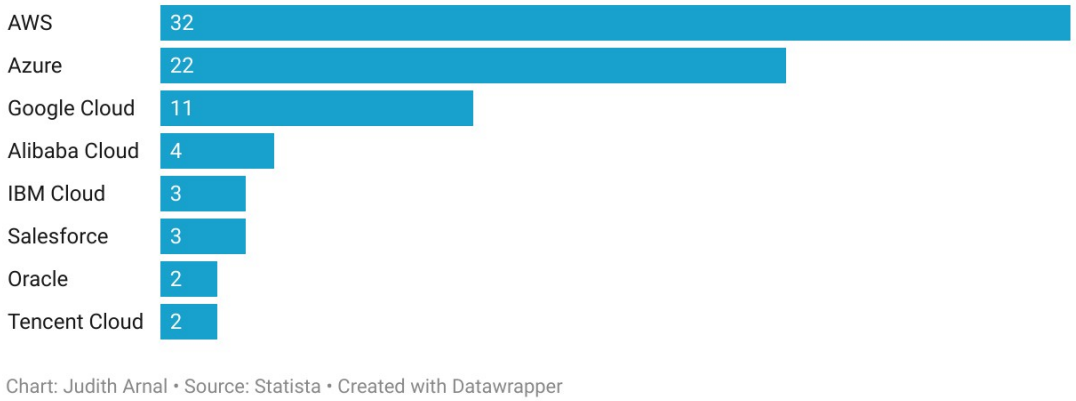
Cloud computing also entails challenges and risks, however. To begin with, and depending on the infrastructure architecture chosen, there's the risk of concentration and vendor lock-in. As shown in Figure 1 below, Amazon Web Services, Microsoft Azure and Google Cloud had a market share of more than 60 % in Q2 2023. This risk calls for action both on the user's side, by assessing the architecture that would best fit their needs, and by cloud providers, by fostering open source technology and multi-cloud approaches which facilitate portability and interoperability.

Second, the lack of trained staff is an ongoing challenge, as making decisions on whether to move to the cloud (and, if so, which functions to move), as well as which strategy to follow in the most optimal way, requires new and technical knowledge that is not easily sourced in the current job market.

Third, regulation's slower progress with respect to technological developments may also pose obstacles to deploying this technology.

Finally, the growing importance of this technology may also alter the nature of the operational risks to be managed (e.g. in terms of data localisation).

Figure 1. Global share of cloud providers (%) in Q2 2023



Source: https://www.datawrapper.de/_/CBjxF/

Cloud technology is increasingly relevant for the banking sector, which has prompted a regulatory response

The banking sector has not remained on the sidelines of cloud computing's growing relevance. Changes in consumer demands, as well as the need to reduce costs and increase efficiency, are leaving banks no choice but to embrace digital change and – in many cases – begin their journey up to the cloud.

THE BANKING SECTOR HAS NOT REMAINED ON THE SIDELINES OF CLOUD COMPUTING'S GROWING RELEVANCE. CHANGES IN CONSUMER DEMANDS, AS WELL AS THE NEED TO REDUCE COSTS AND INCREASE EFFICIENCY, ARE LEAVING BANKS NO CHOICE BUT TO EMBRACE DIGITAL CHANGE AND – IN MANY CASES – BEGIN THEIR JOURNEY UP TO THE CLOUD.

The Financial Stability Board concluded in a 2019 report that cloud computing did not pose an immediate risk to financial stability. At the time, financial institutions' use of the cloud for critical services was limited, with the exceptions being email and risk modelling. But a few years have since gone by and the use of the cloud is now very clearly on the rise. Public authorities are aware of this and are working from a regulatory and supervisory viewpoint to mitigate risks while enabling an efficient use of this technology.

In the EU's case, this has translated into the Digital Operational Resilience Act (DORA). Though DORA entered into force on 16 January 2023, it will only apply from 17 January 2025. DORA aims to harmonise operational resilience rules for the financial sector, applying to 21 different types of financial entities in areas such as ICT risk management, ICT incident management and reporting, testing of the operational resilience of ICT

systems, and the management of ICT third-party risks. Cloud computing falls precisely within the latter category. Indeed, DORA has introduced a framework to oversee the risks posed by the financial sector's reliance on ICT third-party service providers (including for the cloud), as well as a supervisory framework at EU level for said third-party providers.

Following DORA's provisions, European Supervisory Authorities (ESAs) are preparing a set of policy products to be presented in two batches – the first batch by 17 January 2024 and the second by 17 June 2024. In the specific case of third-party risk management, the ESAs are expected to publish three policy contributions[1].

Moreover, the ESAs publicised their joint response to the European Commission's Call for Advice on 29 September 2023, specifying further criteria for critical ICT third-party service providers and determining oversight fees levied on such providers. In relation to the criticality criteria, the ESAs have proposed 11 quantitative and qualitative indicators along with the necessary information to build up and interpret such indicators following a two-step approach.

Myths and realities of supervisory practices of the migration of services to the cloud by the banking sector

Even if DORA is not yet applicable, there is not a legislative vacuum. For the banking sector, the European Banking Authority's Guidelines on Outsourcing Arrangements are applicable, combined with national regulatory regimes[2]. A number of myths have been circulating when it comes to the supervisory practices of cloud services usage by the banking sector – and refuting them is highly relevant.

First myth: the banking supervisor will not allow banks go to the cloud. This is not true, and good proof of this is the existence of 'neobanks', i.e. banks that are 100 % digital, without physical branches, that operate entirely through apps or the web, and that in many cases are already born entirely within the cloud. Another example of this is the ongoing migration to the cloud that many traditional banks are undertaking for at least some of their banking services.

Second myth: the banking supervisor has generally given its approval of cloud usage by banks. This is also false, as operations are analysed on a case-by-case basis. Regulation requires banks to have an outsourcing policy approved by the Board and that it's

[1] For 17 January 2024, two pieces are expected, namely (1) implementing technical standards (ITS) to establish the templates for a register of information and (2) regulatory technical standards (RTS) to specify the policy on ICT services performed by a third party. For 17 June 2024, it's expected that RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function will be published.

[2] In the case of Spain, for instance, this is Rule 43 of the Bank of Spain's Circular 3/2022.

reviewed every two years. In the outsourcing policy, entities must compare their cloud providers with market alternatives, analyse the provider's continued presence in the market, its reputation and economic viability, and taking into account outsourcing chains, as well as defining an exit plan so they can switch providers or relocate cloud services back to their own premises.

Through the outsourcing policy, banks are expected to identify the specific outsourcing risks covered by the regulations, such as the level of concentration and dependence on a provider, outsourcing (also known as 'fourth party risk'), the risk that the outsourcing provider requires financial support, operational and technological risk, reputational risk and/or the risk of breach of contract, among others. Once mitigated, residual risk should be aligned with the financial institution's risk appetite.

Third myth: the banking supervisor must be notified of all services that are moved to the cloud. This is also incorrect – the banking supervisor does not need to be notified of everything that's moved to the cloud, with notification of critical outsourcing being sufficient. Significant institutions will notify the ECB and less significant institutions will notify National Competent Authorities at least two months before the institution starts using its preferred cloud service. The procedure is one of non-objection, meaning that after two months from the official notification, silence will be treated as tacit acceptance and the institution will be able to start using the service.

The documentation required by the supervisor is very broad in nature, but the contract between the institution and the provider, the service level agreements, the institution's outsourcing policy, as well as evidence of its approval, the general and specific risk analysis and the exit plan are particularly relevant.

Additionally, the contract between the institution and the provider is required to cover a number of clauses, such as the right of access and audit by the financial institution and supervisors, the right of termination and exit, notification of incidents (e.g. malicious attacks, data breaches), notification of material changes (such as changes in which regions the provider operates in) or notification of changes in the outsourcing chain. The supervisor allows the submission of a draft contract, but once signed, it must be submitted by the bank within 15 days.

Fourth myth: banks migrate their services to the cloud overnight. This is absolutely not true, at least for banks that conduct a proper risk assessment and carefully plan, especially when it comes to critical services.

In short, it's not a big bang, but a gradual migration. It's usual to start with a pilot phase, continue with a project phase and only if everything has gone well, move on to the production phase. Also, it's important to note that migrating services to the cloud is a shared responsibility between the bank and the service provider. Even though the bank

delegates the service to the provider, it cannot abdicate risk responsibility – this must remain within the bank. It's therefore essential that bank and supplier work as a real team and that both employ professionals specialised in the field.

Risk mitigation practices by banks, cloud service providers and supervisors

The risks types of counting on an on-premise or cloud model are essentially the same, e.g. in terms of information security, fraud or service continuity. But the difference is risk governance, as in the cloud, a number of tasks are delegated by the bank to the cloud provider. In this respect, it's important to determine what the bank will be responsible for and what the cloud service provider will be in charge of.

Based on this, the risk control framework will have to be designed, as the bank will have to set up mechanisms to monitor the responsibilities taken up by the cloud service provider. The risk framework will need to consider the change in the bank's risk profile during its cloud adoption journey.

For the bank, an adequate control mechanism should be based on three lines of defense. The first consists of developing technical and operational measures for the services that the bank intends to move onto the cloud. These measures must comply with the control objectives set by the second line of defense. The second line of defense must independently assess whether the measures proposed by the first line of defense actually meet the control objectives. The third line of defense would be based on the work of the bank's internal auditors. However, as more and more services are outsourced to the cloud, the control system should become more generalised, reflecting not only the risk control of individual initiatives, but also the risk control of technology strategies as a whole.

Also from the bank's perspective, it's worth mentioning a new type of audit, known as a 'pooled audit', which was first included in the EBA's cloud recommendation, and then incorporated into the outsourcing guidelines (not only for the cloud but for all services). The rationale for this type of initiative is that it's difficult for a bank to audit a company of a certain complexity and size. In addition, there is a clear core of common services between the different banks. Because of this, banks wishing to do so could join forces, benefiting not only themselves, but also the cloud service provider itself, which would see its role greatly simplified as the audit's recipient.

The cloud service provider should do everything within their power to ensure the bank exercises control. There are many complementary mechanisms to facilitate this. On a regular basis, websites can be provided to the bank so that it can be fully aware of the current status of services at all times, on top of a quarterly review of the Service Level Agreement (SLA). If incidents occur, best practice indicates that the service provider

should produce a report explaining what has happened, how it reacted and what measures will be taken to prevent a recurrence. For one-off events, such as the Black Friday sales peak, where it's likely there will be a strain on services, advanced preparations can and should be made.

Regarding the supervisor, the expectation is that the bank is aware that delegating tasks is not the same as delegating responsibility, and therefore the bank's risk management framework, which should not provide any blind spots, is of paramount importance.

The banking supervisor's tasks – pending DORA's implementation – are complex, as direct supervision of the cloud service provider is not currently planned. Oversight can only be carried out through the contract signed between the bank and the cloud service provider, but this is not without legal complexities and capacity hurdles. Once DORA is implemented, technology providers that qualify as critical to the European financial sector can be supervised directly at EU level (and not Member State level).

The most relevant risks – the inappropriate use of availability zones/regions and 'vendor lock-in'

Among all the risks identified, two particularly stand out: the risk arising from the inappropriate use of availability zones (and regions[3]) and the risk known as 'vendor lock-in'.

A region is a grouping of availability zones, and in turn an availability zone is a grouping of data centres in a given geographical area, often a very large area. The maximum distance between availability zones is defined so that if there is a natural disaster, such as an earthquake, it does not affect more than one zone. At the same time, the distance between zones should not so great as to cause dysfunctionalities or latency. Each zone has its own sources of power, water, cooling, etc. so that if there is a problem in one zone, it does not spread and affect the entire region.

Obviously, the more regions or availability zones a bank has contracted, the lower the risk of any incident negatively affecting its services. But of course, the bank will incur higher operational costs. Therefore, to make the decision as to how many regions or availability zones to contract, the bank has to analyse the criticality level of the service to know what is required to back up the service in the case of an incident.

As far as the banking supervisor is concerned, the bank is expected to make the decision according to the assessed level of criticality and on it possessing the relevant information from the provider on how the regions and zones are defined.

Then there is the risk of vendor lock-in, i.e. the possibility of being trapped in a contractual relationship with the cloud service provider, especially if it concerns a critical service. This

[3] It should be noted that availability zones and regions are not homogenously defined in the cloud industry.

is why it's so important from a supervisory perspective that the bank has a comprehensive exit strategy in place, minimising any residual risk.

In this sense, the cloud service provider's collaboration is essential and should be seen from two perspectives: first, the provider should allow the bank to exit to another provider; and second, services and tools that can help with this should be provided. Logically, it's much easier to port simple applications than complex ones, thus utilising container architecture could contribute to portability.

Therefore, to optimise portability, which is not an overnight process, several factors must be taken into account. These include minimum permanence times required by the provider party to the contract, whether the user licenses do or do not allow the use of services from another provider, the architecture used (that could possibly minimise migration costs), and implementation standards. In any case, portability should be planned from the outset to avoid some cloud-providing companies from purposely working towards retaining as many customers as possible by minimising exit barriers, an issue that is as common in this sector as in any other.

Cloud is an opportunity for banks to focus on their core business, and a reason to avoid unwarranted protectionist measures

Cloud services are a clear opportunity for banks to free themselves from having to actively manage their most operational and technological issues, thus allowing them to focus on the core of what has always been their business – raising finance and granting credit.

CLOUD SERVICES ARE A CLEAR OPPORTUNITY FOR BANKS TO FREE THEMSELVES FROM HAVING TO ACTIVELY MANAGE THEIR MOST OPERATIONAL AND TECHNOLOGICAL ISSUES, THUS ALLOWING THEM TO FOCUS ON THE CORE OF WHAT HAS ALWAYS BEEN THEIR BUSINESS – RAISING FINANCE AND GRANTING CREDIT.

It is therefore crucial to avoid any unwarranted protectionist measures that could hinder technological progress in the financial sector. While EU companies are indeed heavily reliant on third country companies for the provision of critical cloud services, this reliance needs to be assessed against the European Commission's Economic Security Strategy, which calls for a distinction in assessing dependencies according to the country involved. If the EU is to achieve the targets of the EU Digital Decade, there's no question that cooperation and reliance on strategic partners is needed.

For sure, this does not mean the EU should stop working to foster its own digital environment and EU cloud providers in particular. Ideally, cloud providers to EU banks (and other businesses) would be EU companies.

Nevertheless, given the gigantic challenges the EU is facing in the digital field, balanced measures should be adopted. In this regard, any 'Buy European' clauses or any badly designed European Cybersecurity Certification Scheme for Cloud Services (EUCS) would lead to unwarranted protectionism and would probably hinder EU digital progress by increasing the risk of companies using out-of-date technology. This would, among other things, ultimately damage the competitiveness of the EU banking sector.

Conclusions

Cloud technologies are here to stay and will become increasingly important. Though some specific risks have arisen, such as risk frameworks that don't consider the changes in the bank's risk profile during its cloud adoption journey, as well as concentration or vendor lock-in risks, these nonetheless seem to be manageable. All in all, cloud doesn't appear to be any riskier than on-premise approaches, especially if they're adequately managed.

DORA's swift and adequate implementation is of utmost importance. As pending policy tools are approved and as DORA starts to be actively applied, there should be further analyses to assess the effectiveness of the new framework… but for now, that's a task for another day.

CEPS
Place du Congres 1
B-1000 Brussels