9 JULY 2019

2nd EBF CLOUD BANKING CONFERENCE

Introduction to the work of the EBF Cloud Banking Forum

1 Who takes part in the Forum?

The EBF Cloud Banking Forum focuses on specific regulatory developments related to cloud technology. The forum fosters the much-needed exchange of IT architects, legal experts and cloud specialists from national banking associations, over 15 banks and Cloud Service Providers (CSPs). Leading CSPs' trade associations and EU authorities (European Commission, EBA, ECB) are acting as observers.

The initial dialogue started with partners including Amazon Web Services, Google, Microsoft, OVH and Salesforce. Over time, more industry input was welcomed and the EBF Cloud Banking Forum expanded its reach by including additional players such as Aruba, IBM and Oracle.

Pooling this expertise, the Forum is working on key recommendations in relation to the necessary supervisory framework in Europe. This will help relevant authorities in Europe to understand the specifics of cloud computing for the financial industry and will provide the context when implementing a framework for cloud use by financial institutions in the EU Member States.

Julian Schmücker – Policy Adviser Digital (j.schmucker@ebf.eu, +32 2 508 37 44)

EUROPEAN BANKING FEDERATION AISBL
Brussels Avenue des Arts 56, 1000 Brussels, Belgium, +32 2 508 3711,info@ebf.eu
Frankfurt Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register ID number: 4722660838-23

2 What is cloud and why do banks use it?

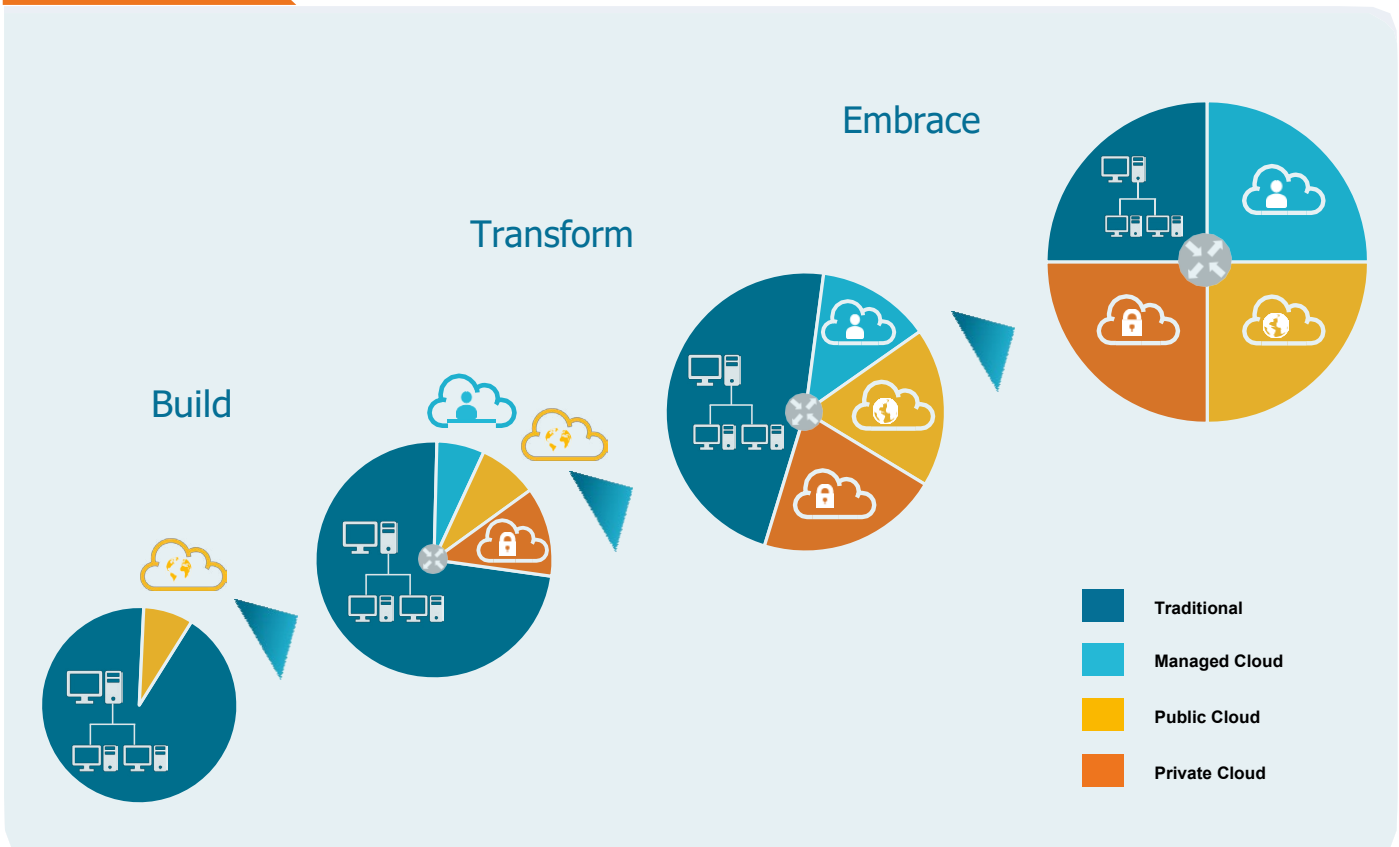
Cloud technology allows industries to tap into new service models, using its technological advancement for new and better services to customers, while improving the flexibility, efficiency and costs of internal business processes. Ultimately, cloud computing can provide a foundation for the digital transformation of the industry in question.

There are several different types of cloud. Private cloud solutions are located inside the banks' own perimeter and as a result leverage all established controls of the respective bank.

Public cloud solutions are located outside of a bank's perimeter and therefore the bank will not operate all controls itself. Hybrid doud is a cloud computing environment using a combination of private cloud (the starting point for most banks) and public cloud solutions that may include third party SaaS (Software as a Service) offerings. These platforms are connected through automation and orchestration tools.

The migration from on-premise IT solutions to cloud is a conscious and careful journey for banks. It starts with an evolution of the existing IT structures and services of banks. Gradually, private cloud solutions can be built, transformed into cloud model combinations and finally embraced in a diverse environment.

FIGURE 1



There are several strategic drivers behind the increased use of cloud by banks, beyond the technological improvement and agility that cloud brings. Examples are:

EFFICIENT USE OF RESOURCES

Cloud computing offers much more flexibility than traditional IT systems. Traditionally, banks have had to operate IT systems with excess capacity to deal with the highest volumes of activity foreseen, such as peak trading levels on financial markets. Very often this excess capacity remains unused despite costs incurred for building and maintaining it. Cloud solutions offer banks the flexibility to tailor the scaling up of capacity to meet their activity levels, ensuring a much more efficient use of resources in a secure environment.

MORE EFFECTIVE USE OF BANK CAPITAL - FROM CAPITAL TO OPERATIONAL EXPENDITURE

Traditional IT infrastructure requires large upfront investments (capital expenditure) by banks. The current prudential rules of CRD/CRR disincentivise the investment that banks make in software assets owing to the obligation to fully deduct them from Common Equity Tier 1 capital. This in turn can require banks to raise additional funds to make the necessary investments. By contrast, using cloud services provided by CSPs can be more effective as the costs will be categorised as an operating expense and not a capital expenditure, thereby leading to a reduction of required capital when deploying new services.

STATE-OF-THE-ART SECURITY

In most cases, CSPs have stronger security than most individual companies can maintain and manage on-site. Moreover, the big cloud service providers have large teams of security engineers and, given that cloud is (one of) their core businesses, they are continuously investing in meeting the strictest and newest security standards.

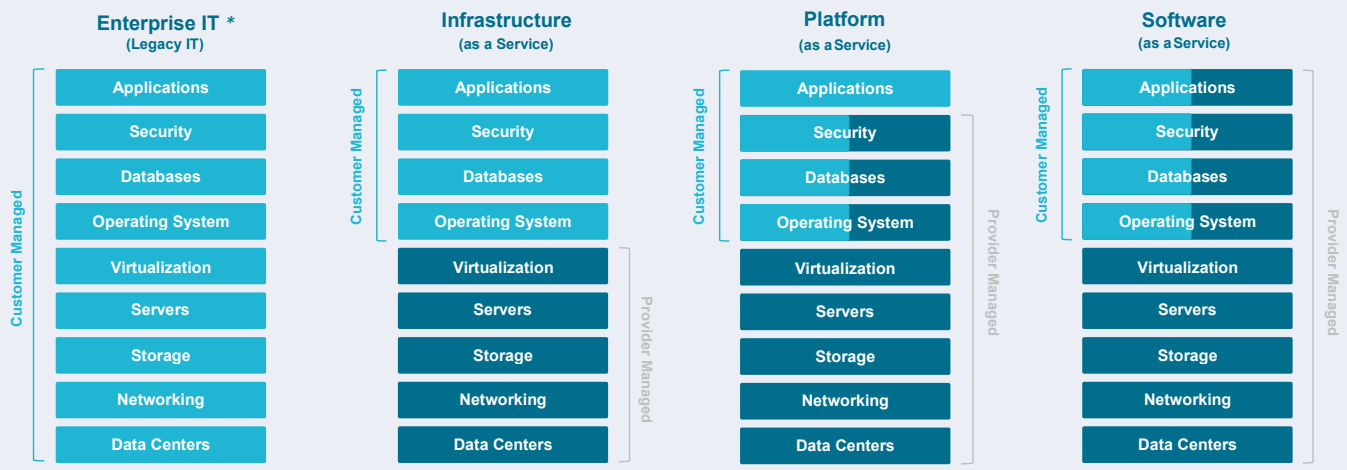
> “cloud solutions offer banks the flexibility to tailor the scaling up of capacity to meet their activity levels”

3 Adopting Cloud – a risk-based approach

The adoption of cloud solutions by a bank is a journey during which it will assess the risk, control demand and the control mechanisms it has at its disposal. These vary depending on the type of cloud solution. Figure 2 serves as an exemplary illustration.

Like any function outsourced to a third-party provider, the outsourcing of activities through the hybrid or public cloud brings some form of operational risk which needs to be carefully managed. The operational risk occurs both during the adoption phase (migration to the cloud) and the operational phase (operation of cloud services). At any stage, the accountability of the bank remains unquestioned.

FIGURE 2[1]



*If operated by the own entity

Cloud service models are different from other IT paradigms. Regardless of the type of cloud solution, banks show necessary awareness of differences such as the control demand, facilitated by an assessment based on five risk metrics:

ONE - The layer of abstraction: depending on the solution, the bank will have a different level of control over the process and applications, either running its own process or relying on those of the CSP.

TWO - Ownership of the control framework: this examines the degree to which the control framework of the cloud solutions remains with the bank or with the CSP.

THREE - Legal and regulatory context: the jurisdiction governing the cloud solution, the activity supported by the cloud solution (e.g. handling of personal data) and the location of the data will have an influence on the balance of controls between the bank and the CSP.

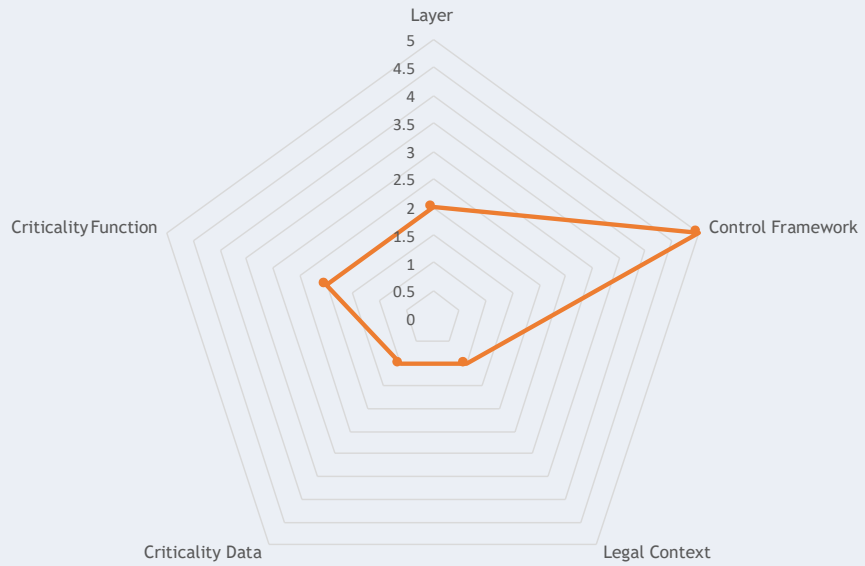
FOUR - Data criticality: different categories of data can be identified that have different levels of sensitivity. Sensitive customer personal data requires higher protection than public machine generated data, for example used to calculate intraday risk.

FIVE - Criticality of function: This dimension outlines how dependent the day to day operation of the bank is on the function relying on a cloud solution. The criticality is reflected in the impact of the function not performing properly. For example, a bank's business processes could run without a HR system for a short period of time. This is not true for the core banking system, which would bring the bank to halt if it is failing.

[1]Based on the figure at: https://mycloudblog7.wordpress.com/2013/06/19/who-manages-cloud-iaas-paas-and-saas-services/. While innovative cloud services constantly evolve, thereby preventing an exhaustive and static overview, this simplified visual will help to understand the distinction between management features according to cloud services in question.

These metrics allow for a specific assessment for each separate cloud solution, illustrated by figure 3. The exemplary assessment applies numerical value (from 1 to 5) to each of above's dimensions, in order to support the visualization for the purpose of awareness:

FIGURE 3



Layer	2
Control Framework	5
Legal Context	1
Criticality Data	1
Criticality Function	2

4 Cloud adoption - need for a harmonised approach

The possibility for banks to adopt cloud is of vital strategic importance and will significantly contribute to the aspiration of the EU to show digital leadership and expand the digital economy further. It will also allow banks to deliver innovative digital solutions to customers.

To that end it is essential that EU institutions, the European Banking Authority (EBA) and National Competent Authorities (NCAs) develop a harmonised and coherent approach to cloud solutions and their adoption by banks. This requires a shared understanding of risks and particularly a shared approach in terms of information, requirements and the reporting that is expected from banks.

To contribute to this effort, one of the initial workstreams of the EBF Cloud Banking Forum has been at work to produce guidance to banks on how to comply with the new reporting requirements that come into effect as part of the 2019 EBA Guidelines on outsourcing arrangements (which replace the 2017 EBA Recommendations on outsourcing to cloud service providers). The EBF Cloud Banking Forum looks forward to continuing its work in close collaboration with its EU observers and other regulators, to ensure useful and consistent reporting without creating an unnecessary administrative burden on banks. Detrimental effects caused by fragmentation across the EU shall be prevented.

Another workstream of the EBF Cloud Banking Forum has focussed on developing a common understanding of the expectation banks have in terms of cloud exit strategies and, more specifically, the testing of exit plans.

The work has particularly focussed here on reaching a consensus on possible testing methods of a table-top test:

- Review of the technical viability of the exit plan by technical subject matter experts;
- Review of the exit plan against existing enterprise capabilities by the IT service owner;
- Review of the exit plan against current organisational security standards for protection of data at rest and in transit to verify adequacy of planned controls;
- Calculation of current data volumes and identification of the impact on data transfer requirements;
- Calculation of costs and timing implications of identified changes;
- Review of agreements and collaboration procedures between the institution and Cloud Service Provider related to removing outsourced functions and data from the service provider to ensure continued adequacy if deviations are identified;
- Walkthrough of the plan with exit plan participants;
- Desktop exercise - having the participants of the exit plan discuss the plan in theory, and checking whether it is useable in a passive exercise room environment;
- Simulation, verifying the robustness of procedures and operating assumptions in a fully monitored and controlled environment by testing the effectiveness of a plan in support of a theoretical response to a scenario.

5 A peek into the future

The work of the EBF Cloud Banking Forum does not stop with the delivery of the technical papers on:

THE USE of cloud computing by financial institutions

THE REGISTER under the EBA Guidelines on outsourcing arrangements (cloud-specific guidance for banks)

CLOUD EXIT STRATEGY – testing of exit plans

These papers will be used to exchange with the EU observers in the EBF Cloud Banking Forum. They will continue to be assessed and updated as the use of cloud solutions, and the regulatory requirements related to it, continue to evolve. The Forum looks forward to engaging with its EU observers and other regulators to ensure that guidance, such as reporting requirements, meet the policy goals behind them while avoiding fragmentation across the EU.

After its 2nd Cloud Banking Conference, the EBF Cloud Banking Forum will further reflect on the areas where additional recommendations and joint understandings would be appropriate, considering for example proportionality, the assessment of outsourcing arrangements and governance frameworks in line with the 2019 EBA Guidelines.

Julian Schmücker – Policy Adviser Digital (j.schmucker@ebf.eu, +32 2 508 37 44)

EUROPEAN BANKING FEDERATION AISBL
Brussels Avenue des Arts 56, 1000 Brussels, Belgium, +32 2 508 3711,info@ebf.eu
Frankfurt Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register ID number: 4722660838-23