Are banks really ready for Cloud?

Are banks in Europe ready to move to public clouds? Or is it all a pipe dream? The banks and their consultants finally talk.

A report by ActiveViam.

ACTIVEVIAM

Contents

- Introduction and Methodology 3
- Executive Summary 4
- Public cloud budgets for 2018: are they a myth? 5
- Compliance: is it the biggest threat to public cloud adoption? 6
- The great use case debate: do public clouds carry too much risk to handle bank risk? 7
- A new hiring profile: who will lose or gain jobs in banks as a result of public cloud migration? 8
- Conclusion 10

Introduction

In the wake of the European Banking Authority's (EBA) published **guidelines on how to outsource and supervise cloud environments effectively**[1], ActiveViam, an in-memory analytics company, conducted research with some of the world's top banks and their consulting partners to determine a number of things:

1. Are public cloud projects in banks on the rise? If yes, why?
2. What are the main factors stopping public cloud projects going ahead in banks?
3. Which use cases are banks moving to public clouds?
4. What do public clouds mean for banks' hiring strategies?

In gaining opinions from industry leaders, as well as predictions from individuals within the banks, ActiveViam is able to understand whether public cloud projects are really happening in 2018, or if they are simply a pipe dream swallowed up by other priorities.

Methodology

ActiveViam interviewed customers and partners in the banking sector between October 2017 and December 2017, across Europe. ActiveViam also interviewed candidates in the US for additional commentary on the use of public clouds in banks, and opinions on the European Banking Authority's recent initiative.

The types of roles the interviewees hold include "Head of Risk IT", "Head of Risk", "Head of Market Risk" "CTO", "President" "Technical Architect" "Technology Director".

The types of banks interviewed include major financial institutions in Europe, such as UBS, as well as members of the Big Four.

Definitions

Public cloud is cloud infrastructure where physical machines are shared (concurrently and subsequently) between customers, depending on their requirements and usage.

Private cloud is cloud infrastructure where the use of physical machines is exclusive to a single client or institution.

On-site hardware refers to the collection of infrastructure, such as servers and storage, that is used and owned by banks at their various office locations throughout the world.

1. https://www.eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf

Executive Summary

1. Public cloud budgets for 2018 are not a myth

Some banks are rapidly increasing their use of public clouds in 2018, so much so that banks' IT budgets are increasing by up to 70% in the next two years to cope with the initial spin-up fees. Up until now, many banks have not catered for public cloud usage within IT budgets, meaning the demand is initially high for hardware rental, as certain public cloud projects get underway.

2. GDPR and general compliance are the biggest obstacles to public cloud

The dangers posed by data leaks and general compliance challenges, including complying with the General Data Protection Regulation (GDPR) are still defined as the biggest threats preventing public cloud migration, with over half of interviewees stating compliance.

3. The great use case debate: risk-related use cases are being closely evaluated for public cloud projects

Recently, the European Banking Authority (EBA) released Recommendations to banks for supervising outsourced cloud projects, **including guidance on data processing and auditing**.[2] The one issue banks are still struggling to determine, despite the guidelines, is which use cases are suitable for public cloud. In our survey, 64% of respondents believe we will see more risk-related use cases migrated to public cloud from the banks, such as Market Risk and Counterparty Risk.

Interestingly, 40% respondents believe there is no use case just suitable for private cloud, which opens up more opportunities for use cases involving Personally Identifiable Information (PII) and sensitive company information.

4. You're hired! Banks are looking for new skills as a result of public cloud projects

The traditional installer and network roles are getting re-tooled. Banks need less installers, and more coders, information security specialists and individuals with service management backgrounds. If traditional infrastructure specialists are willing to adapt their skills, they are likely to move to new roles within a bank. If not, you will see the cloud vendors acquiring these candidates from the banks to help manage the bigger customer accounts.

> "The key thing you need is consensus about what use cases can go into public clouds. That isn't there right now."
>
> **Director at a Big Four firm**

2. https://www.eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf

Public cloud budgets for 2018: are they a myth?

No, they most certainly are not. They are real and are on the rise.

The pace at which public cloud projects are going on varies across the bigger and mid-size banks. Each bank is doing something different. On the whole, respondents believe IT budgets for public cloud projects will rise by 6 to 10% in the next two years, however some individuals inside the banks have stated that certain projects have warranted a budget increase of up to 70%. This may be because they were very low in 2016 and 2017, meaning additional funds are required to cope with the initial spin-up fees.

The chief cause of pressure to migrate to public clouds and invest this budget is cost. Almost all of our respondents have cited cost savings as the main reason for migrating systems to public clouds. That, and digital transformation demands.

If projects are migrated to public clouds, lines of business can control what they need, when they need it and if they need more, while saving money. Operating costs will decrease in banks simply because business units "pay as they go" at the point of demand and decline.

By implication, this changes how business units approach dealing with their technology needs, and IT teams start to operate differently. Cloud projects herald an era of "Bring Your Own Solution", so lines of business can use their own budgets to satisfy hardware demands, without having to receive ongoing approvals from the IT team, which is a long, arduous process.

However, if the line of business receives a level of autonomy from IT, does that put more pressure on internal compliance teams at the banks to keep the lines of business in check?

55% of respondents are already using public cloud services, or are aware of public cloud services being used by another line of business in the bank.

64% of respondents intend to migrate certain systems to public clouds in the next two years, or are aware of their banking clients doing so.

Public cloud budgets are going up by as much as 70% to cope with public cloud spin-up fees.

Compliance: is it the biggest obstacle to public cloud adoption?

The dangers posed by data leaks and general compliance challenges, including the GDPR, are still defined as the biggest threats preventing public cloud migration, with over half of interviewees stating compliance.

Compliance teams are under increasing stress as more data protection regulations come into force. This impedes the progress of public cloud projects in banks for a number of reasons. PII, which is the focus of the platinum-standard data protection regulation in Europe – the GDPR – is arguably at greater risk if stored in public clouds. Or is it? The open nature of public clouds means other banks and the general public can share the same servers, and therefore banks have to relinquish control to the vendors with full liability. But the game is changing.

If there is a data breach and unencrypted PII should leak, local data protection regulators need to determine where the fault lies: at the bank, the vendor, or the vendor's subcontractors. With the GDPR coming into force, there is just as much penalty emphasis on the vendor (the "data processor"), as there is on the "data controller" (the bank). This has not been the case previously: the bank would be fully liable. Because of this change to how data privacy regulations work in Europe, there are equal incentives for banks and their cloud providers to prevent data breaches. In addition, the specific security concerns posed by public clouds have been identified years ago, with cloud vendors often employing some of the world's best cybersecurity and data protection experts to help allay any threats.

Furthermore, as more regulations appear, such as BCBS 239 and MiFid II, compliance hires are becoming more important. A bank's compliance team needs to have eyes across the entire bank, and that will become increasingly difficult if more banks introduce public cloud projects before 2020. Arguably, the majority of our respondents say compliance is the number one priority in 2018 in banks instead of public cloud projects. In all likelihood, once a fully- functioning compliance team is in place, there can be more engagement with public clouds in general. Some interviewees even stated that compliance departments oppose moving anything to the cloud almost systematically because there is too much legal uncertainty.

So, if certain data is preventing the compliance team saying 'yes' to public cloud projects, what use cases might they agree to?

> "Compliance and audit functions need to understand public cloud: how it works and the implications for data, including customer data. A data security team is critical for this."
>
> **Amit Gupta, Executive Director Risk Technology, UBS**

The great use case debate: do public clouds carry too much risk to handle bank risk?

Now public cloud projects are steadily on the rise, and budgets are going up as banks begin to spin up hardware for multiple projects, what are the most common use cases for public cloud? And are there certain use cases that only belong in private cloud?

Across the world, regulators and authorities recognise the trend towards cloud outsourcing in banks. Most recently, the EBA – following the example of other countries such as Singapore – ran a consultation in Europe with a view to providing guidelines on how banks should supervise cloud environments. However, it seems the industry still remains uncertain about which use cases are best for public cloud projects. The resulting guidelines from the EBA do not specify use case recommendations – something which half of our interviewees preferred. So, without formal guidance, will the banks take different paths with regards to which use cases they move to public clouds?

Overall, there is reticence to move PII and sensitive tier one information to public clouds, such as a banks' financial statements and results. Over half of the interviewees felt that tier one data and PII should not be prioritised for public clouds. In theory, this does not sound surprising, considering the regulatory and reputational issues involved. However, at the same time, there is a school of thought suggesting if a use case is suitable for private cloud, it is suitable for public cloud.

> "The reality is most banks go to datacentre providers to find a physical home for all their kit already. Public cloud commoditises all of that a bit more, but it's more or less the same principle."
>
> **Risk IT Architect, International investment bank**

While reluctant to prioritise tier one information for public clouds, there is a tendency towards prioritising risk-related use cases, such as Market Risk and Counterparty Risk to public clouds. For example, over half of respondents believe use cases involving real-time or fast-moving data, requiring a lot of processing power, should be prioritised for public clouds. By implication, certain risk use cases fit this profile.

Risk use cases are huge consumers of infrastructure – banks often have thousands of servers that run grid-compute, meaning they are a good use case for public clouds. If a regulator asks a bank to run more stress scenarios, it can be more elastic and deploy an extra 500 or so servers in the public cloud.

As regulators demand more, and more risk calculations are required to ensure the right decisions are made, the cost savings associated with public clouds are starting to outweigh the risks. This means we will see more use cases hosted in public clouds, but it is unlikely to be anything ground-breaking. There will be deliberate 'baby steps' while banks get to grips with pending regulations. To sidestep the regulations, use cases that do not involve certain data types will be prioritised as the perfect 'guinea pigs' in the next two years, like risk use cases.

A new hiring profile: who will lose or gain jobs in banks as a result of public cloud migration?

During a period of transition in Europe and the UK, banks' overall hiring strategy is under the microscope. Different reports suggest that Brexit means reducing staff numbers in the UK, while others suggest the status quo is to be maintained. Macroeconomic shocks, such as Brexit, are certainly impacting where banks increase or decrease their hiring numbers, but ultimately, if candidates have specialist skills in highly-coveted areas, these shocks do not matter. High-profile bankers have stated publicly that less-coveted roles will need to decrease by significant numbers as certain technology, **such as Artificial Intelligence and Machine Learning offerings, begins to assume the roles of individuals**[3].

As public cloud projects are considered over the next few years, a new hiring profile is starting to emerge. Banks require individuals across a few specific teams – IT, compliance and legal – that understand cloud infrastructures.

It's no secret that, a few years ago, personal computing allowed business users to take control back from the IT team as part of the "Bring Your Own Device" (BYOD) boom. Now, it seems cloud computing is doing something similar. The implicit trade-off here is that an IT department, which has a considerable influence in banks, controlling a sizable fraction of the workforce and budget, will need to adjust to a new working model, developing teams with a broader skillset.

Specifically, on the IT side, the traditional datacentre manager role is set to change, as banks need more commercially-savvy employees who can work with cloud vendors: those that understand pricing models, compliance demands and the needs of each line of business to ensure applications are tenanted to the right place. Over half of our interviewees stated that datacentre managers, network managers, system maintenance and installers will not be needed. If traditional infrastructure specialists are willing to adapt their skills, they are likely to move to new roles within a bank, such as DevOps and Information Security. If not, you will see the cloud vendors acquiring these candidates from the banks to help manage the bigger customer accounts.

So what does this mean for the C-Suite?

> "When applications migrate to public clouds, you have to account for the fact that the infrastructure the apps are running on is considered as code. Individuals with coding and DevOps skills will be in higher demand than those with just the traditional operations skillset."
>
> **Sri Ganesan, Managing Partner, Risk Focus**

> "There will be a change in culture. Clearly you will need much less people to manage the bank's own hardware. However, if people adapt their skills to new architectures, things could still run smoothly."
>
> **Head of Risk IT, Major European bank**

3. http://uk.businessinsider.com/former-citi-ceo-30-of-banking-jobs-will-be-wiped-out-in-5-years-2017-9?r=US&IR=T

It changes things at the C-Suite on a number of levels, mainly because teams are set to change.

The Chief Data Privacy Officer

Heavily-regulated firms, like banks, are hiring Chief Data Privacy Officers and data privacy teams to ensure compliance with data privacy regulations. The consensus from our respondents is that compliance is a bank's top priority for 2018, and considering the pending GDPR, this is no surprise. With more public cloud projects comes an increasing focus on where certain data is. Compliance teams and Chief Data Privacy Officers will need to understand how public cloud and vendor management works, and the implications on specific types of data.

The Chief Risk Officer (CRO)

CROs heavily influence which tools their teams use to manage risk. Cloud computing offers more autonomy in trying out new solutions or mix-and-matching them, especially if the data they work on is already in the cloud in some form. Solution evaluation and deployment is easier for CROs if cloud is involved, and there is a greater control over costs and less reliance on IT. However, it is likely the IT team will limit the providers available to use for cost and practical reasons. Eventually, as more projects move to public cloud, and the approved vendors are chosen, risk teams will have more autonomy moving forwards.

The Chief Operating Officer (COO)

COOs need to be commercially aware about how much infrastructure costs, especially when attributing back to business lines. Infrastructure billing is very complex at the moment for most banks, but public cloud cost attribution makes things a lot more transparent. IT teams will know precisely how to cost projects, forcing business lines to think more commercially about their asks from an IT perspective. This gives more power to the COO, as long as there is an initial level of understanding of cloud infrastructure.

The Chief Information Officer (CIO)

Private clouds have been around for a while, meaning CIOs have been working with cloud providers to run a bank's datacentre needs already. However, with public clouds, if a project needs more infrastructure to run it, a public cloud project can scale it up incredibly quickly, whereas in private cloud more checks need doing to see if certain things are possible. Therefore, with this new level of flexibility, a CIO's team structure will change – and it will become a service management function, with less focus on basic hardware management. This will not happen overnight however, and CIOs will be in charge of overseeing complex, public cloud transformation projects.

The Chief Information Security Officer (CISO)

Before public cloud, the CISO and the CISO's team worked on a physical technology perimeter close to the bank. Now, the perimeter at a bank no longer relies on the network, it relies more on services. With this change, the threat profile of a bank changes, meaning a broader skillset is needed for a CISO's team: such as specialists in intruder detection and endpoint security.

Conclusion

Public cloud projects in banks are happening. They are happening in different ways in different banks. While there are still regulatory challenges, the advantages of public cloud projects are starting to outweigh the risks.

These next three years are critical for global banks. As well as dealing with macroeconomic shocks, the banks are having to change their cultures, change their technologies and change their people, to cope with the demands of a modern world. Public clouds are a step in this long process. Our interviewees do not believe public cloud migration is banks' priority in 2018; instead there was overwhelming consensus towards compliance. That does not mean banks are not increasing their budgets though – what was merely out of the question a few years ago, is now very appealing.

About ActiveViam

ActiveViam provides organizations with instant insight into their operational processes for timely and context-aware decision-making. ActiveViam's analytical in-memory technology, ActivePivot, brings analytical capabilities into data-intensive and time-sensitive business processes including risk management, supply chain management, compliance and CRM. ActivePivot uniquely allows business users to produce, analyze and monitor complex performance indicators in real-time and to extract actionable intelligence from massive amounts of complicated and fast-moving data.

ActiveViam, founded in 2005, is a privately-owned company with offices in Paris, London, New York, Hong Kong and Singapore. It serves customers in various industries including, but not limited to financial services, logistics, transportation, market exchanges and retail.

Contact us

London	+44 20 7836 8820
Paris	+33 1 40 13 91 00
New York	+1 646 688 4442
Singapore	+65 62 24 46 63
Hong Kong	+852 3971 9154

info@activeviam.com