

# CAPCO

**CLOUDY WITH A CHANCE OF CONCENTRATION RISK**

---

Financial services institutions are increasingly using public Cloud Service Providers (CSPs) to host their workloads, and this has not gone unremarked by regulators. As a result, those institutions that have built their strategy on a single strategic public cloud partner have cause to be concerned by new proposals aimed at eliminating concentration risk in this space.

Now is the time for companies to investigate adopting multi and even poly cloud models in order to mitigate concentration risk, and also to revisit and test Business Continuity Plans (BCPs) while looking to place an emphasis on portability and reliability.

The latest policy statement from HM Treasury, issued on June 8, notes that over 65 percent of UK firms are using one of the top four cloud providers to host their workloads. In the Treasury's view, this presents a significant potential systemic risk should any one of those CSPs fail<sup>1</sup>.

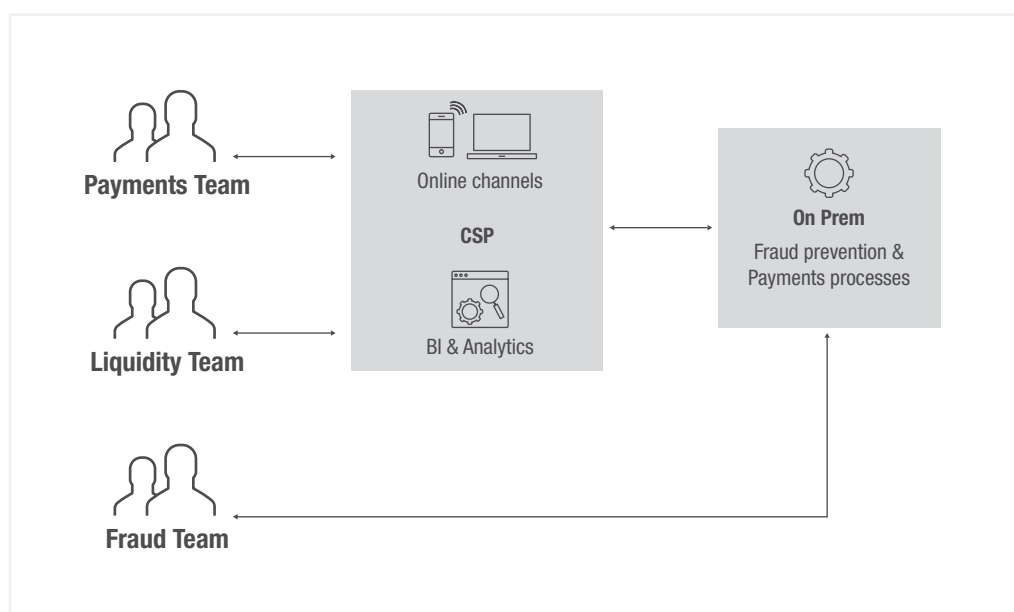
Accordingly, PRA, FCA, Bank of England and HMT will be setting minimum resiliency standards in respect of third-parties, providing services to those elements of the financial sector that have been deemed critical. Although they are not yet stipulating which hosting strategy financial services firms must adopt, they request that mitigations must be in place to ensure those institutions are not tied to just one CSP.

There are a few different hosting strategies on the financial services transformation agenda<sup>2,3</sup>. When choosing one or more CSPs, each strategy should be assessed in four ways. In this article we are going to focus on three – concentration risk, portability, and reliability – and how they can build resilience within your organisation. The fourth – sustainability – will be explored in a future article.

- While the systemic impact of **concentration risk** around critical banking services that is currently so concerning the Treasury and regulators is not the direct responsibility of individual financial service institutions, concentration risk at an organisational level most certainly is. Reducing concentration risk is imperative to increasing resilience in the event of outages at a CSP.
- **Portability** is the ability to move applications and/or data from one CSP to another. To increase resilience against stressed and unstressed exits, organisations would like to seamlessly transfer their services in a variety of failure scenarios. However, increased portability comes with increased cost and complexity, and therefore there is a trade-off when determining the extent of portability required. At the time of writing, the industry is considering a set of tools that allows some degree of portability. At Capco, we are breaking down the portability concern into infrastructure (as a code), business service code and data.
- **Reliability** is particularly prized in the financial services industry, where customers expect services to be online 24/7 and the regulators are increasingly scrutinising cloud resilience<sup>4</sup>. The chosen CSP(s) must demonstrate a high degree of reliability, with next to zero planned down time, and the hosting strategy needs to include back up options either on premises or with another Cloud Service Provider, so they are resilient to outages.

# IN THE BEGINNING THERE WAS HYBRID CLOUD

The hybrid model is the traditional cloud adoption pattern in the financial services industry. For hybrid cloud, a public cloud provider is used in conjunction with private infrastructure or a private cloud for the realisation of business services.



**Figure 1:** Example of a hybrid cloud model where workloads span one Cloud Service Provider and on premises core systems

Hybrid cloud allows organisations to choose what information they store on public cloud vs private cloud and/or private infrastructure, which can be attractive to those storing sensitive data. Conversely, public cloud enables a higher reliability when compared to private infrastructure due to its services being distributed across multiple data centres.

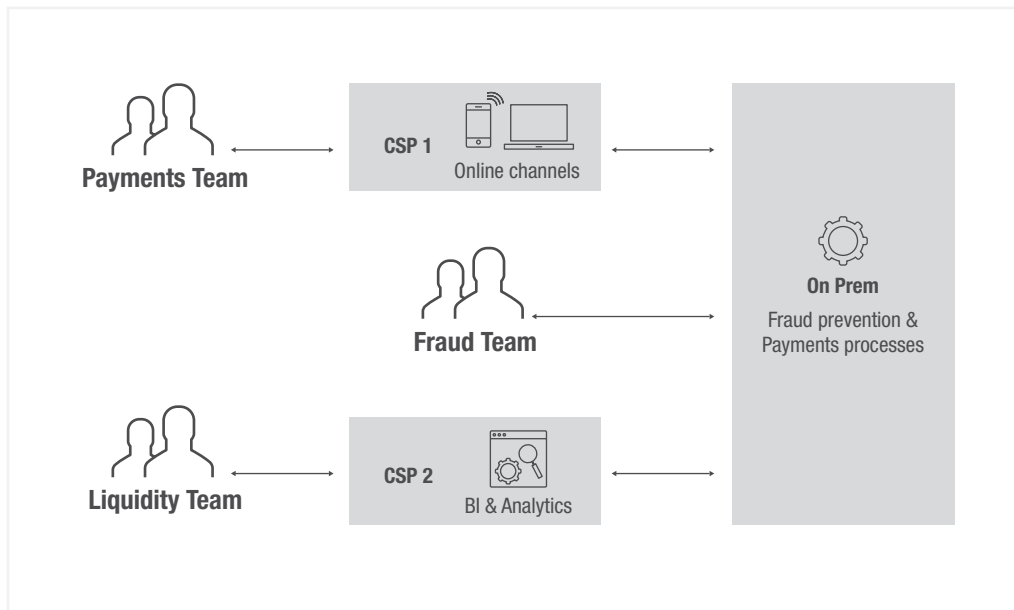
AWS (Amazon Web Services), Azure, and Oracle provide some of their own infrastructure on client premises to allow consolidated infrastructure management. However, on premises hardware must be bought and supported which can be costly.

Portability is often an issue, so organisations must define and test exit plans to allow for relocation of infrastructure, codebase, and data between cloud providers, covering both stressed and unstressed scenarios – e.g. responding to a catastrophic CSP failure or when a commercial relationship ceases.

It also needs predefined capacity for provisioning the infrastructure and increases vendor lock in and concentration risk levels. If for some reason the relationship with the CSP breaks down, your workloads would move back on-premises and you would lose the benefits of the public cloud.

# MULTI CLOUD TO THE RESCUE

The accumulation of concentration risk and the spectre of vendor lock-in has driven most financial service organisations to seek an alternative hosting strategy. For **multi cloud**, multiple cloud providers are used for the same technology capabilities depending on business service workload.



**Figure 2:** Example of a multi cloud model, where a different cloud provider is used depending on the business service workload. Here the payments channels workloads are on CSP (Cloud Service Provider) 1 while business intelligence and analytics channels are on CSP (Cloud Service Provider) 2. Payment processing happens on premise.

Currently, multi cloud strategies offer the most in terms of reliability and portability, e.g., ensure that secure connectivity is in place between on premise datacentres and both CSPs. With workloads spread across cloud providers, concentration risk and vendor lock-in are reduced, easing transition should a CSP have a more attractive offer. Reliability is also increased, as an outage at one CSP would not impact workloads hosted on another CSP, thus reducing the outage blast, and only impacting one user group.

However, multi cloud requires a skilled workforce who can manage multiple CSPs, and cross cloud monitoring, or cost control might become a challenge. The added complexity can add to costs not only to training and hiring talent, architecture and solution design, security, observability, operations, and governance (comparable with poly cloud strategy).

Whilst the issue of concentration risk is somewhat mitigated, cloud providers are extending their offering, providing more sophisticated services such as advanced machine learning, artificial intelligence or blockchain

# ALONG CAME POLY

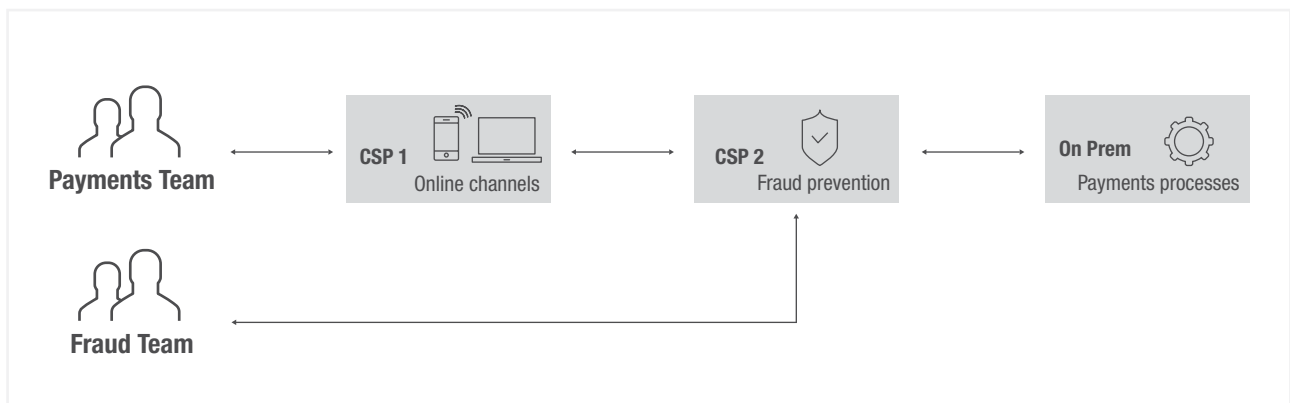
The **poly cloud** model is the latest evolution of cloud strategy and promises performance optimisation through the decoupling of services across cloud platforms.

For poly cloud, the CSP service pair is intentionally chosen to fulfil a specific business service workload, meaning that the services are decoupled across CSPs (i.e. multiple providers per workload). This differs from hybrid where only one provider is used and multi, where the services are not decoupled across providers (i.e. one provider per workload).

The main advertised advantage of poly cloud is the access to performance/ efficiency gains by choosing the best tool for the job.<sup>4</sup> Rather than compromising and using one CSP across the workload, organisations can take advantage of specialist offerings per service within the workload.










Given this attractive proposition, many organisations might be tempted to adopt this novel approach. However, poly cloud poses several challenges from reliability angle. Each additional CSP used increases the chance of experiencing outages. Looking at some of the main cloud providers between January and March 2022, GCP (Google Cloud Platform) had 23 incidents<sup>5</sup> and Azure had 9<sup>6</sup>. Whilst most incidents were not considered major, the cumulative impact could be large should your services be decoupled without failover options.

For example, in Figure 3, if either CSP1 or CSP2 were down the whole workload would fail while in multi cloud only one Cloud Service Provider is relied upon per workload.



**Figure 3:** Example of a poly cloud model where workloads are decoupled across Cloud Service Providers (CSPs). Here fraud prevention and payments processes are decoupled so that online channels are hosted in CSP (Cloud Service Provider) 1, but the services are hosted in CSP (Cloud Service Provider) 2 and on premise.

# IN SUMMARY

STRATEGY	CONCENTRATION RISK	PORTABILITY	RELIABILITY
<b>HYBRID</b>	<b>Increased:</b> Blast radius in case of CSP outage will impact all cloud-bound flows 	<b>Limited:</b> Porting back on premise is difficult especially in PaaS (Platform as a Service) scenarios or when on premise infrastructure is scaled down 	<b>Increased,</b> assuming high availability setup 
<b>MULTI</b>	<b>Lower,</b> e.g. by equally distributing important business services between two cloud providers 	<b>Improved:</b> Network connectivity between on premise and both cloud providers are in place along with CI CD pipelines and skills 	<b>Equivalent to hybrid cloud</b> 
<b>POLY</b>	<b>Equivalent to hybrid cloud</b> 	<b>Equivalent to multi cloud</b> from CI CD and skills perspectives 	<b>Lower:</b> In case any CSPs have an outage, the entire business service will be impacted 

A multi cloud strategy allows more flexibility in choosing the right CSP to host your workloads and an opportunity to lower concentration risk levels. Additionally, it allows seamless exit scenario testing and business continuity plans enabling infrastructure, code, data, and state portability by design.

To prepare for any failure scenarios and to increase reliability, you need:

A secure connection between on premise and two or more cloud providers readily available CI/CD pipelines

- Foundational cloud technologies in place
- Infrastructure as Code scripts
- Reusable well tested patterns and standards.

In practice, therefore, despite the potential for increased operational and observability complexity, we believe that multi cloud is the best trade-off when considering the balance of **concentration risk**, **portability**, and **reliability**. We also

recognise that a small number of specialised use cases might require a poly or hybrid cloud. Moreover, it offers most of the building blocks so it can be seen as an accelerator for any other use case.

## WOULD YOU LIKE TO TALK TO US ABOUT YOUR CLOUD ADOPTION STRATEGY?

Whether you are on cloud adoption day zero, have already begun to migrate workloads or wish to overhaul your current cloud strategy, we would like to talk to you. We can help you with:

- Alternative Cloud Service Provider selection
- Workload placement strategies
- Concentration risk assessments and mitigation
- Building cloud adoption accelerators
- Strategic domain design

# REFERENCES

---

1. HM Treasury [Online] <https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement#fn:3>
2. O'Reilly. [Online] <https://www.oreilly.com/library/view/what-is-polycld/9781098104634/ch01.html>.
3. Colocation America. [Online] <https://www.colocationamerica.com/blog/poly-cloud-vs-multi-cloud>.
4. Deploy flow. [Online] <https://www.deployflow.co/single-multi-or-poly-cloud/>.
5. Google Cloud Service. [Online] <https://status.cloud.google.com/summary>.
6. Azure. [Online] <https://status.azure.com/en-us/status/history/>.

# AUTHORS

**Corneliu Rimboiu**, Principal Consultant

**Jessica Bevan**, Senior Consultant

# CONTACTS

**Peter Kennedy**, Partner  
[peter.kennedy@capco.com](mailto:peter.kennedy@capco.com)

**Corneliu Rimboiu**, Principal Consultant  
[corneliu.rimboiu@capco.com](mailto:corneliu.rimboiu@capco.com)

**David Cecil**, Managing Principal  
[david.cecil@capco.com](mailto:david.cecil@capco.com)

**Jessica Bevan**, Senior Consultant  
[jessica.bevan@capco.com](mailto:jessica.bevan@capco.com)

**Lawrence Aggleton**, Managing Principal  
[lawrence.aggleton@capco.com](mailto:lawrence.aggleton@capco.com)

---

# ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at [www.capco.com](http://www.capco.com), or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

# WORLDWIDE OFFICES

## APAC

Bangalore  
Bangkok  
Gurgaon  
Hong Kong  
Kuala Lumpur  
Mumbai  
Pune  
Singapore

## EUROPE

Berlin  
Bratislava  
Brussels  
Dusseldorf  
Edinburgh  
Frankfurt  
Geneva  
London  
Munich  
Paris  
Vienna  
Warsaw  
Zurich

## NORTH AMERICA

Charlotte  
Chicago  
Dallas  
Hartford  
Houston  
New York  
Orlando  
Toronto  
Tysons Corner  
Washington, DC

## SOUTH AMERICA

São Paulo

**WWW.CAPCO.COM**



© 2022 The Capital Markets Company (UK) Limited. All rights reserved.

JN\_4404

**CAPCO**  
a **wipro** company