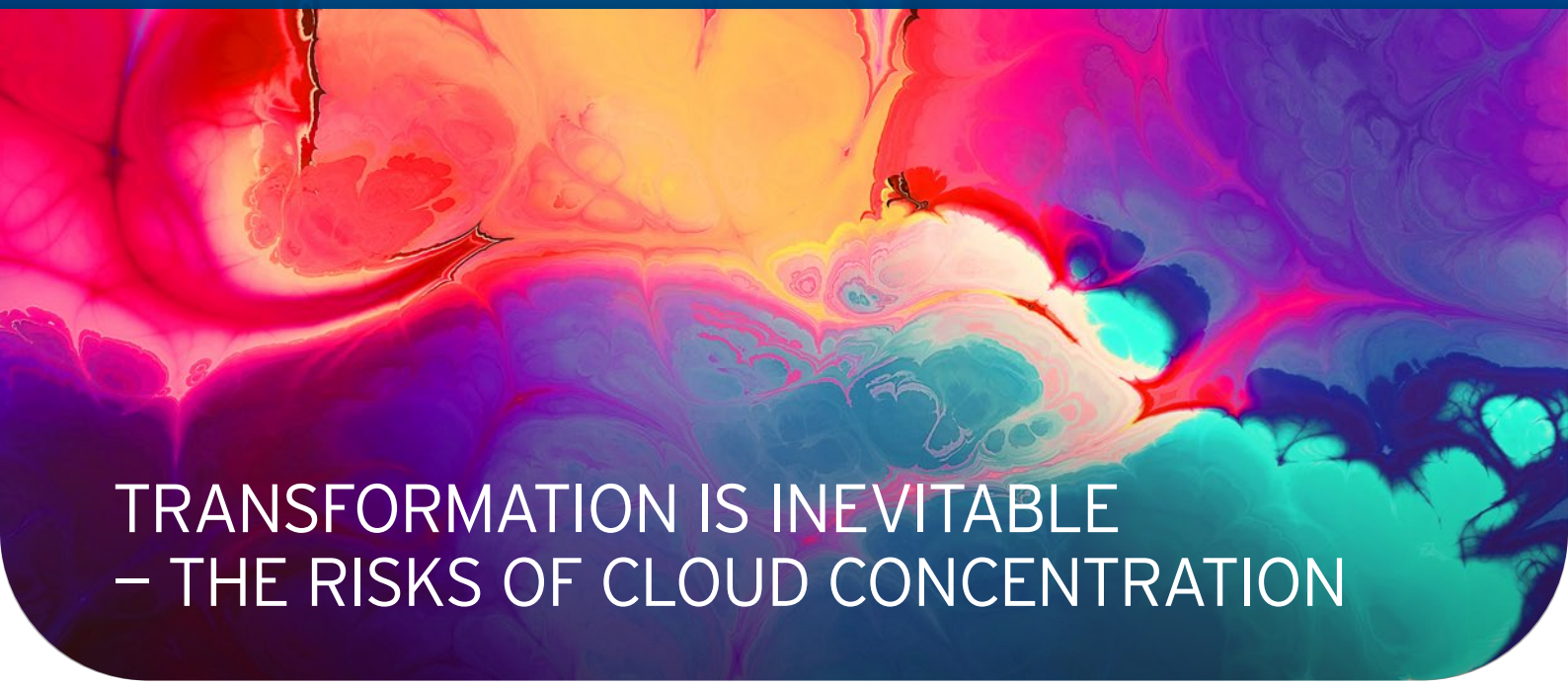


TRANSFORMATION IS INEVITABLE – THE RISKS OF CLOUD CONCENTRATION

Welcome to the latest article in our 'Transformation is inevitable' series, where we provide insights based on our on-going analysis of the complex, changing and ambitious regulatory policy environment, evolving customer and employee needs, as well as advancing technology.

In our first two articles we looked at the future of work and sustainable finance,[1] and the possible future direction of UK regulation now that the UK is no longer part of the European Union.[2]

In this, our third article, we look at the potential risks that may arise from the ever-increasing use of cloud outsourcing.

A brief history of the cloud

Cloud computing isn't new. It can trace its origins back to the 1960's and the development of mainframe computer systems that were sophisticated enough to enable multiple users access to different applications at the same time, through the combination of pre-programmed utilities, virtualisation[3] and networking. This meant that organisations could utilise expensive computers[4] in a more efficient manner.

Initially limited to networks contained within a single building or campus, the development of the internet, more sophisticated telecommunications, and the World Wide Web led to servers being located remote from users, not just in another building but in another city or even another country.

However, in the late 1970s, the advent of comparatively cheap desktop computers that were capable of managing their own operating systems, utilities and storage, lessened the need for central processing with servers reduced to data storage and networking.

This trend began to be reversed in the first decade of the 21st century with the launch of Amazon Web Services (AWS) and Google Docs in 2006, heralding the rebirth of shared infrastructure under its new name; the cloud.

AWS, developed using the extensive infrastructure Amazon had built for its own online presence, offered a number of web-based services to users including Amazon Elastic Compute Cloud (EC2), which allowed users to rent virtual server capacity, and Amazon Simple Storage Service (S3) which charged users for storing data. Google Docs began to offer similar services, extending them to home users through free to use word processing and other office tools.

This growth in data storage and the provision of cloud utilities requires vast amounts of computing power. Whereas users require nothing more than an internet connection and a device capable of accessing the web, cloud service providers (CSPs) need vast data centres and server farms to ensure their products meet the needs of their clients. For example, AWS has around 38 datacentres spread between the US and Europe. These datacentres will each house thousands of servers.

The vast infrastructure needed to operate a cloud service does not come cheap, so it's no surprise that the market is dominated by firms such as IBM, Oracle, and SAP as well as, what is known as, the GAFAM: Google, Apple,

Facebook, Amazon and Microsoft. These companies are big. Really big. According to the European Securities and Markets Authority's (ESMA) Report on Trends, Risks and Vulnerabilities No.2 2021, the GAFAM have a combined market capitalisation of EUR7.2 trillion, that's around 23% of the S&P 500 in H1 2021[5] with IBM, Oracle and SAP accounting for around a further EUR500 billion.

The new concentration risks

Regulators understand the benefits of outsourcing, including to the cloud, noting that it can lead to lower costs, fuel innovation and allow firms to adapt to the digital economy. They even acknowledge that the cloud could potentially enhance operational resilience compared to in-house information communication technologies (ICT) infrastructure.[6]

However, the concentration of cloud provision with a limited number of providers has begun to raise alarm bells, with regulatory bodies such as the Bank of England expressing the view that the increased reliance on a small number of CSPs has the potential to be systemically important and that a failure by one or more of these providers could lead to long-term damaging effects to financial markets.[7]

And it's not only the direct exposure to CSPs that can cause concern. CSPs have their own dependencies, for example to hardware suppliers, that can ultimately impact their clients. At the time of writing there is a global shortage of semiconductors, the silicone chips that have found their way in to almost all consumer electronics, from toasters to Teslas. If this continues the limited supply could impact CSPs' ability to scale up their platforms to cater for increasing demand, with CSPs competing for the same limited resources, not just against each other but against firms maintaining their own, more traditional, ICT infrastructure.

Global regulator notes growth in third-party dependencies

In December 2019, the Financial Stability Board (FSB) published a report on third-party dependencies in cloud services that explored potential issues for supervisory authorities and financial stability stemming from the scale of services provided via the cloud and the small number of globally dominant CSPs.[8]

In its analysis of potential risks of cloud services, the FSB stated that a significant failure of a CSP was unlikely due to their high technological and physical resilience, but failure is not impossible.

The FSB went on to state that overall there were no immediate financial stability risks stemming from the use of cloud services by financial institutions (FIs). However it noted the potential for this to change in the future, especially if FIs increased their exposure to cloud services.

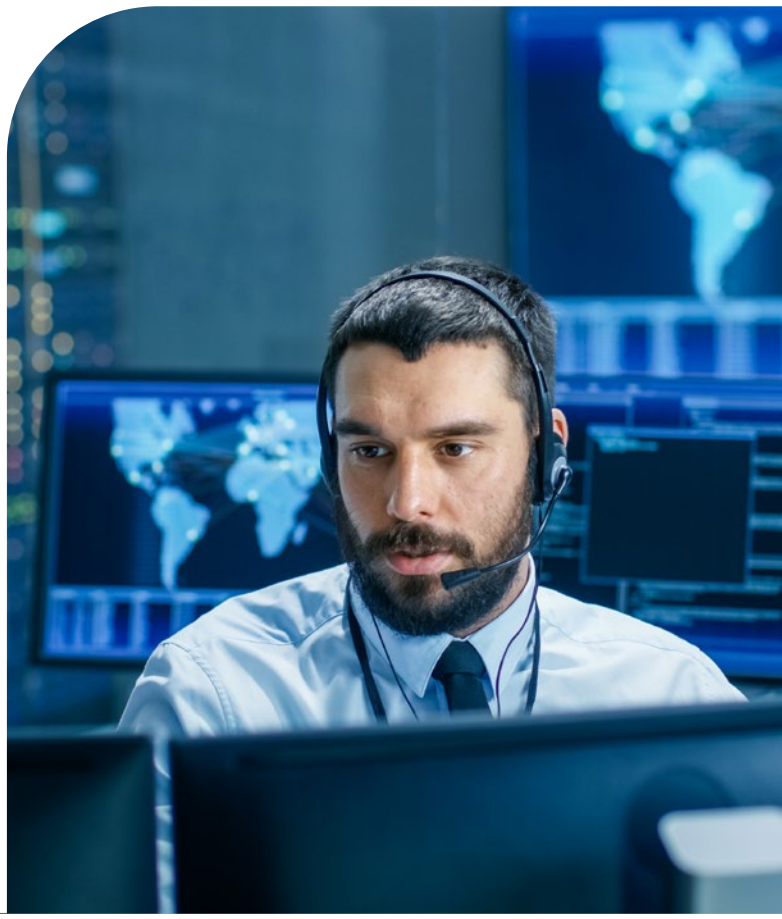
However by November 2020 the FSB's opinion appeared to be changing. In its discussion paper on regulatory and supervisory issues relating to outsourcing and third-party relationships, the FSB included concerns expressed by national supervisory authorities about possible systemic risks arising from concentration, and the need for enhanced dialogue between supervisory authorities and third-party providers so that market participants understand the system-wide effects of outsourcing.[9]

Regulatory approaches are evolving

Prior to the COVID-19 pandemic, regulators' concerns for concentration risk focused on an individual firm's exposure to a single third-party that undertakes multiple functions and the risks associated to the failure of that provider to the firm alone.

This was not because the regulators didn't recognise the risks associated with the concentration of services into a small number of service providers but because, as the UK Financial Conduct Authority outlined in its *guidance for firms outsourcing to the 'cloud' and other third-party IT services*, originally published in June 2016, if concentration risk were to relate to the risk of many firms using the same service provider, it would be difficult for firms to be aware of and monitor, due to likely confidentiality restrictions.[10]

So, at least one regulator was aware of the risks but felt that, at that time, firms didn't have the ability to assess them.



Five years down the road however and the COVID-19 pandemic appears to have focused regulators' views on monitoring CSPs, and they have become increasingly concerned about the confidentiality and security of data, operational resilience, and cyber risks that could, in theory, spread more quickly through shared systems.

Just how concentrated is the cloud market? As of Q1 2021 it is estimated that AWS, Microsoft Azure and Google accounted for 58% of the total cloud market with AWS having 38% market share alone.[11]

Behind this is the unprecedented increase in cloud usage since March 2020. In its Bulletin No.37, the Bank for International Settlements quoted a survey that indicates that 82% of companies increased cloud usage as a result of the COVID-19 pandemic, with more still to come as firms get used to the new normal of hybrid working and greater reliance on ICT, artificial intelligence based tools, etc.[12]

With this background in mind, regulators are introducing or adapting rules and guidance to help firms put in place operational resilience processes and procedures and take control of their relationships with CSPs, as well as taking steps to monitor them and their impact on markets directly.

In Europe, ESMA's *guidelines on outsourcing to cloud service providers*, published in December 2020, includes requirements for national competent authorities to identify and monitor concentration risks and to evaluate both their potential impact on the firms they supervise and the stability of the financial market.[13]

Although these guidelines only apply to UCITS managers and AIFMs, they align with similar requirements published by the other European Supervisory Authorities (ESAs), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Banking Authority (EBA).

In addition to the guidelines issued by the ESAs, the European Commission is currently formulating rules that will require all participants in the financial system to have safeguards in place to mitigate against cyber attacks and other risks.

Additionally, the EU's Digital Operational Resilience Act (DORA) has been designed to ensure a sound monitoring of ITC third-party risk.[14] This should be achieved through the implementation of principle-based rules and by harmonising the key element of the service and relationship with CSPs. The proposals go as far as to include a detailed description of what must go into the contract between the firm and the CSP.

Looking globally, in October 2021, the International Organization of Securities Commissions (IOSCO) updated its principles for certain regulated entities that outsource tasks to third parties.[15]

The IOSCO principles are technology neutral, in that they do not differentiate between CSPs and other outsource providers, however IOSCO makes it clear that CSPs present risks that must be addressed as part of a firm's due diligence and oversight of outsource service providers.

The consultation that led to the Final Report presented the findings of a survey IOSCO undertook, during 2017, into the use of cloud services by credit rating agencies. The survey was undertaken so that IOSCO could better understand how outsourcing integrates with cloud computing, and how outsourcing and cloud computing are used by firms and incorporated into their organisational strategies and structures.

Although the principles do not directly apply to asset managers, IOSCO has stated that it is "keeping a watching brief" on the application of outsourcing principles to asset management.

Not a one-sided exercise

Fortunately this is not a one sided exercise, with several CSPs recognising the importance of ensuring that their clients have full access to the information required by regulators. As a result they have devised tools intended to aid firms in meeting these demands.[16]

The exponential growth of data

Data protection is also a concern where unimaginable amounts of personal data are held by a small number of CSPs. The amount of data accumulated by social media alone is astronomical, for example in 2014 it was estimated that Facebook generates four petabytes of data per day.[17] That's roughly equivalent to taking 16,000 digital photos. Every day. For the rest of your life.[18] Not only must CSPs protect this data from external attack, but they must also ensure data is ring-fenced within the shared infrastructure they operate.

Intellectual property must also be protected. Users of the cloud are not limited to just data storage and may use the products on offer by CSPs to develop new, innovative products and services. The CSPs must ensure that they have processes in place to protect the data and intellectual property of their clients and those end users have a responsibility to satisfy themselves that they are protected.

Areas of developing regulation

One of the problems regulators see with outsourcing to CSPs is that these are large, unregulated companies that are often based in other jurisdictions and not directly captured by relevant regulations.

To counter this, regulators are increasingly including extraterritorial requirements to their regulations.

For example, the European Union's 2018 General Data Protection Regulation applies to any company holding data in relation to European citizens, regardless of where that company is located. DORA will have similar requirements.

In Hong Kong, the Securities and Futures Commission (SFC) has gone further still. In October 2019 it issued a circular on the use of 'external electronic data storage' which details the restrictions placed on Hong Kong firms using cloud service providers and other delegated data storage providers.

The key requirements include:

- Approval by the SFC to use external data storage.
- A requirement that the location of data storage is:
  - Physically in Hong Kong; or
  - Where data storage is undertaken outside Hong Kong, the outsourcing firm must obtain a obtain a written agreement from the cloud service provider that it will comply with all requirements of the SFC to access the data held by it and provide access to staff members of the cloud service provider who have technical knowledge of its data storage or information systems if required.
- The data held cannot be transferred to another data storage facility.

In addition to these rules, the SFC published a report on operational resilience and remote working arrangements on 4 October 2021.[19] This report details the SFCs observations following supervisory discussions with licenced corporations during the COVID-19 pandemic.

In addition to the observations, the report also lays down operational resilience standards and required implementation measures which supplement the SFC's existing guidance.

Globally, both IOSCO and the FSB stress the need for cross-border cooperation between both regulators and CSPs to address potential systemic risks and ensure market stability.

Just how likely is a CSP to fail and what impact could this have?

On 4 October 2021 we got a taste of what could happen when Facebook, Instagram, WhatsApp, Facebook Messenger, and Workplace, which are all owned by Meta (the company formally known as Facebook) and share the same ICT

infrastructure, stopped working. For around six hours users were unable to access the applications, affecting not only individuals wanting to post pictures of their lunch but companies that depend on Facebook's products to do business. Facebook admitted responsibility for the failure, the result of 'a faulty configuration change', and has stated that it will work to understand what happened so it can make its infrastructure more resilient.[20]

Is this the end of the beginning?

The use of outsourcing and ICT by the financial services industry has changed since the 1960s, with the two rapidly coming together and, in some respects, becoming indistinguishable from each other over the last decade.

The COVID-19 pandemic has accelerated the take up of cloud services, a trend that doesn't look like abating even as we slowly return to the office.

As firms hand over more functions, and more data, to a small number of CSPs, so regulators globally are taking action to increase their ability to oversee the operation of these behemoths.

So far this has involved adapting existing rules and guidance; ensuring the cloud is included in outsourcing oversight requirements and introducing an extraterritorial aspect to new rules.

But could regulators go even further? The Financial Stability Institute (FSI) seems to think so. In a speech to the fintech working group at the European Parliament, delivered on 16 June 2021, Fernando Restoy, Chair of the FSI, suggested that big techs (large technology firms such as IBM, Amazon, etc.), especially those that offer key services such as cloud computing, could be subject to comprehensive regulation encompassing all their activities, much like the way banks are regulated.[21]

So far the cloud has been a source of silver linings for the financial services industry. It has introduced efficiencies and stimulated innovation. But as more and more firms transfer their ICT infrastructure to the cloud, the risks of systemic failures increases.

It's up to regulators, CSPs, and the firms that outsource to them to make sure those happy clouds don't become a storm.

[1] See https://www.citibank.com/mss/solutions/pfss/solutions/fund/fiduciary-services/assets/docs/how-can-citi-help/Transformation_is_Inevitable_Vista_for_AMs.pdf.

[2] See https://www.citibank.com/mss/solutions/pfss/solutions/fund/fiduciary-services/assets/docs/how-can-citi-help/Transformation_is_Inevitable_No2.pdf.

[3] Virtualisation uses software to simulate hardware functionality. This allows for multiple users to simultaneously work off the same physical server. The benefits include greater efficiencies and economies of scale.

[4] In 1961 the IBM 1401 mainframe, promoted as the first affordable general purpose computer, could be rented for USD2,500 a month – equivalent to almost USD23,000 today. Even at that price IBM installed over 12,000 machines, nearly half of all the computers in the world at that time.

[5] See ESMA Report on Trends, Risks and Vulnerabilities No. 2 2021 at www.esma.europa.eu.

[6] An example of these views can be found in the introduction the FSB discussion paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships at www.fsb.org.

[7] See Dear CEO letter – Supervisory expectations in relation to material outsourcing to the public cloud dated 17 September 2021 at www.bankofengland.co.uk.

[8] See Third-party dependencies in cloud services Considerations on financial stability implications at www.fsb.org.

[9] See Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships at www.fsb.org.

[10] For an example see FCA guidance for firms outsourcing to the 'cloud' and other third-party IT services (FG16/5) at www.fca.org.uk.

[11] See ESMA Report on Trends, Risk and Vulnerabilities at www.esma.europa.eu.

[12] See BIS Bulletin No.37 – Covid-19 and cyber risk in the financial sector at www.bis.org.

[13] See Guidelines on outsourcing to cloud service providers at www.esma.europa.eu.

[14] See COM (2020) 595 final at eur-lex.europa.eu.

[15] See Principles on Outsourcing Final Report at www.iosco.org.

[16] For an example see the AWS and the European Banking Authority Guidelines on Outsourcing at aws.amazon.com.

[17] Facebook's Top Open Data Problems at research.fb.com.

[18] Petabyte – How Much Information Could it Actually Hold? at info.cobaltiron.com.

[19] See Report on Operational Resilience and Remote Working Arrangements at www.sfc.hk.

[20] See Update about the October 4th outage at engineering.fb.com.

[21] See Regulating fintech: is an activity-based approach the solution? at www.bis.org.

Please contact for further details:

David Morrison
Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
+44 (0) 20 7500 8021

Ann-Marie Roddie
Head of Product Development Fiduciary Services
annmarie.roddie@citi.com
+44 (1534) 60-8201

Amanda Hale
Head of Regulatory Services
amanda.jayne.hale@citi.com
+44 (0)20 7508 0178

Caroline Chan
APAC Head of Fiduciary Business
caroline.mary.chan@citi.com
+852 2868 7973

Shane Baily
EMEA Head of Trustee and Fiduciary Services
UK, Ireland and Luxembourg
shane.baily@citi.com
+353 (1) 622 6297

Jan-Olov Nord
EMEA Head of Fiduciary Services
Netherlands and Sweden
janolov.nord@citi.com
+31 20 651 4313

CBS36023 11/21