Google Cloud

Executive summary

Google Cloud appreciates the efforts of the Federal Stability Board (FSB) to outline Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships and the opportunity to respond to the Discussion paper. Over the past several years, we have seen increased regulatory focus on harmonising the approaches to third-party outsourcing and risk management, including in the cloud context. Having a consistent and unified view at the global arena, that the FSB is best placed to define and champion, is critically important.

As financial institutions (FIs) embark on their digital transformation journey all over the world, including in the view of the challenges brought on by the COVID-19 pandemic, we believe that clear and enabling principles for firms to use cloud services are key to regulators' overall objective to protect investors, ensure market integrity, and maintain financial stability.

Financial institutions are greatly benefiting from cloud technology in a multitude of ways to understand risk, segment customers, develop new instruments and ultimately offer better and more innovative products to their consumers. Thanks to the cloud, financial institutions can quickly process large volumes of information, reducing their time to market, and providing more agility and scalability at a lower cost. Capital markets firms can also utilise the cloud to combat fraud and money laundering through artificial intelligence (AI) and machine learning (ML) models. Similarly, cloud-based technologies are being leveraged for firms' risk-management to determine liquidity and exposure quicker, carry out mark-to-market adjustments and for more effective regulatory reporting. These benefits are fundamental to the industry transformation and need to be accounted for in the regulatory guidance.

FIs are choosing to use cloud services because they find the cloud to be equally or more secure and resilient than their existing, often legacy, computing infrastructure. The advancement and competition of cloud technologies in the last few years provide firms with data protection, data analytics, and operational resiliency capabilities that are more advanced than what individual organisations, especially SMEs and smaller firms, can develop on their own. This in turns could lead to protection for investors and financial stability.

We welcome the FSB general recognition of the benefits of cloud-based services in the Discussion paper. We also understand and acknowledge regulatory concerns over the challenges of concentration risk, third party dependencies and supply chain management - in the context of outsourcing to cloud providers, and here below share our view on the potential mitigants.

We remain at your disposal for further discussion, and believe that a coordinated global dialogue on these issues could be further facilitated by the FSB to bring together the perspectives of the national regulators, financial institutions and third party providers in a constructive multi-stakeholder forum.

Google Cloud

Detailed response

1. What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

Despite the continuous and very welcome regulatory effort in many jurisdictions to harmonise and unify definitions and guidance to critical third party outsourcing, including in the cloud context, implementation and supervisory practices remain highly fragmented across the globe, even within the same geographical markets. In our experience, this is caused by (1) lack of industry best practice (2) the level of technical cloud-specific expertise available to the supervisors.

To address these challenges of fragmentation, it would be beneficial to have an **global, principled based, risk assessment framework** shared between financial institutions and cloud providers, that could be developed - potentially under auspices of the FSB. Alternatively, global certification schemes for the use of cloud services in the financial sector could be a meaningful avenue to explore.

Other risks and barriers include:

- Lack of regulatory coordination at the global level - both from supervisory and policy perspectives as multiple outsourcing and operational resilience regulatory frameworks emerge across the globe;
- Assumptions of the risks of cloud outsourcing - in many proposed regulatory frameworks, the approach to cloud outsourcing is focused on the assumed augmentation of risk arising with the use of third party services whilst in reality migration to public cloud helps increase cybersecurity and operational resilience capabilities of the FIs; gaps in understanding of the technological reality of cloud services often lead to disproportionate regulatory requirements;
- Data localisation and sovereignty requirements that prevail in many regulatory approaches, in particular in APAC and the EU, are in many cases incompatible with the nature of cross-border digital innovation and global trade; more narrow and pragmatic approaches based on risk-assessment and mitigations are needed to achieve the right level of controls and stability protections in a meaningful way;
- Disproportionate and prescriptive security requirements deviating from a principles and risk based approach (eg data segregation requirements; overly prescriptive encryption requirements etc) are problematic as they can in fact increase (not reduce) the risks.

In the context of outsourcing to cloud service providers, we understand the regulatory focus on the following three areas outlined in the Discussion paper:

1) Third-party dependencies in cloud services and associated risks of concentration, vendor lock-in and perceived digital operational resilience and stability challenges triggered by over-reliance on a single provider;

Google Cloud

2) Access, audit information rights and associated challenges of potentially restricted regulatory access to third-party providers;
3) Supply chain management and supervisory expectations on sub-outsourcing risk management, including in the view of the additional complexities brought to life by the COVID-19 pandemic.

Third-party dependencies and technological operational resilience
Whilst FIs need to consider all the risks attendant to the activities that they outsource and prepare the appropriate mitigants and management plans as part of their due diligence and in conjunction with their third party providers, it is important to bear in mind that in general these risks (eg security, resilience, etc) are the same as the risks that the firms need to manage in a non-outsourced model. Indeed, certain of these risks may be easier to manage when outsourcing to specialist providers (*such as cloud hyperscalers as migration to public cloud can greatly improve firms' technological operational resilience and security capabilities - not augment the risk*), given the providers' ability to invest in technology, technical and geographical scale and skills.

The key risks to consider are those that can disrupt the dependencies (i.e., people, technology, facilities, third parties) that underpin the firm's business services:

- **Cybersecurity** Continuously adjusting key controls, people, processes and technology to prevent, detect and react to external threats and malicious insiders.
- **Pandemics** Sustaining business operations in scenarios where people cannot, or will not, work in close proximity to colleagues and customers.
- **Environmental and Infrastructure** Designing and locating facilities to mitigate the effects of localised weather and infrastructure events, and to be resilient to physical attacks.
- **Geopolitical** Understanding and managing risks associated with geographic and political boundaries between intragroup and third-party dependencies.
- **Third-party Risk** Managing supply chain risk, and in particular of critical outsourced functions by addressing vendor lock in, survivability and portability.
- **Technology Risk** Designing and operating technology services to provide the required levels of availability, capacity, performance, quality and functionality.

Overall the security capabilities that are offered by hyperscale cloud providers have largely surpassed those available on premise, which is broadly recognised by the global financial services industry and regulatory authorities. In fact cloud's **ability to augment security and reduce the risk** is largely seen today as one of the reasons why regulated industries are accelerating their transition to the cloud[1]. From this perspective, financial institutions need to evaluate their cloud strategy with a focus on how their risk management processes can be improved with cloud functionality.

[1] See McKinsey, Making a secure transition to the public cloud, 2018

Google Cloud

Case Study: Security and operational resilience at Google Cloud

Security protections and resilience of public cloud can be more robust, scalable, and cost-effective than legacy systems available on-premise to organisations individually (especially smaller organisations).

Throughout the COVID-19 pandemic Google Cloud has not faced, nor do we foresee, any shortfalls in our network, compute or customer support capacity. All our technical and personnel readiness steps implemented in response to the pandemic are from our standard playbooks, which were written and have been tested for exactly this type of scenario, well ahead of the crisis. This is strong evidence of how transition to the public cloud can help improve operational resilience and security - not increase stability risks.

In addition to building-in security, Google designs our systems to be highly resilient. Google's data centres are geographically distributed to minimise the effects of regional disruptions, such as natural disasters and local outages, on global products. Within each data centre all hardware and software components are redundant and network traffic is load balanced.

Google pioneered the concept of Site Reliability Engineering (SRE), an engineering discipline focused on the reliability and maintainability of large systems that is now used widely in the industry. Teams of SREs within Google monitor tools and systems to ensure they're performing properly, identify and correct failures, and develop improvements that make these systems faster, more cost-effective, more efficient, and more reliable.

Google also conducts regular (weekly to monthly) operational practice tests, where incidents are simulated and need to be responded to appropriately, with minimal service disruption. The operational team is thus trained through practice and procedures are kept up to date to maintain a high level of operational readiness. Beyond team-level activities, Google also exercises disaster recovery (DiRT) company-wide to ensure coordination across products and to measure the response effectiveness.

Certain other risks are presented through the use of outsourcing, in particular the risks associated with the service provider being unable, for any reason, to provide the contracted services. When considering cloud service providers, we believe that the implementation of cloud services that are based on open source and open cloud principles, gives firms the best mechanism to manage such risks, because it enables portability of workloads between different cloud providers (multi-cloud) and on-premise (hybrid cloud).

As the Discussion paper points out, financial institutions and their regulators are increasingly focused on operational resilience aspects of third party outsourcing, reflecting the growing dependency that financial services firms have on complex systems, automation and technology, and third parties. There are a number of definitions of operational resilience provided by regulators including:

Google Cloud

> *"the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions."*[2]
>
> *"the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."* [3]
>
> *"the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality"*[4]

What is common in these definitions is the approach of seeing operational resilience as an *outcome* that is achieved through the effective management of risks that may prevent the ongoing operation of important functions. From this perspective, the approach presented by the Bank of England, PRA and FCA UK in their 2019 Consultation papers on operational resilience (PRA CP29/19 - Operational resilience: Impact tolerances for important business services[5] and FCA CP19/32 - Building operational resilience: impact tolerances for important business services and feedback to DP18/04[6]) is particularly innovative and future proof, and is well versed to be further considered as a best practice at the international level.

The approach to the forthcoming operational resilience policy introduced by the UK regulators in these papers is grounded in the recognition of the view that *failure is inevitable* and needs to be planned for and learnt from as an important step of operational resilience planning. Therefore firms need to ensure that they are testing the effectiveness of their response with an understanding of failures on one hand, and the provisions for continuation of their important business services and recovery regardless of a failure on the other. Such policies will be a step-change in how the supervisory authorities regulate firms' approach to operational resilience at large.

It is important that FIs consider *all* of the risks that may prevent their ongoing operation, rather than taking a narrow approach and/or assuming that operational resilience is effectively a different term for business continuity planning.

---

[2] "Operational resilience: Impact tolerances for important business Services" Bank of England CP19/29
[3] "Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC
[4] "Draft Regulation on digital operational resilience for the financial sector", European Commission
[5] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf
[6] https://www.fca.org.uk/publication/consultation/cp19-32.pdf

Google Cloud

As part of establishing the levels of operational resilience that a firm requires, it will often determine what its 'failure tolerance' is for a given business service, using a range of severe but plausible scenarios. In some locales this differs definitionally from 'risk appetite' and is designed to identify the point at which specific thresholds will be crossed, for example:

- Market impacting: the point at which there is an adverse effect on the wider financial services ecosystem;
- Customer impacting: the point at which significant harm is done to customers of financial services firms.

Defining 'failure tolerance' using these external reference points reflects regulators' intent to strengthen the operational resilience of the sector as a whole. In other words, *the point at which a firm's failure damages the market or harms customers*, may be different to *the ambitions a firm may have regarding operational resilience as expressed by its risk appetite*.

Why is it important that the business service, with its defined failure tolerance (or risk appetite), is the starting point for managing operational resilience? Because it ensures that the *outcome* is what is right for the customer, firm and industry, rather than the outcome being an expression of levels of resilience that are available with today's technology, people, facilities and third parties.

Access and audit rights

Whilst we understand the perceived challenges over regulatory access to critical third party providers, we would challenge the common assumption that all cloud providers tend to impede these customer and regulatory rights or not cooperate with the supervisory requests. At Google Cloud we are fully committed to transparency and supporting customer compliance with their regulatory requirements. Audit rights are provided for in many regulatory guidances globally, including the FFIEC in the United States, the MAS in Singapore, the APRA in Australia and EBA, ESMA and EIOPA requirements in Europe and **Google Cloud consistently facilitates audits by our regulated customers, their supervisory authorities and their appointees**. This commitment is equally acknowledged in our Financial Services contract. Google has facilitated a number of customer audits including two pooled audits by the Collaborative Cloud Audit Group (CCAG) and a regulator-led audit in 2019. In many cases regulators have started to expressly acknowledge and address the specific considerations when conducting audits in a multi-tenant environment, including by encouraging FIs to ensure they do not unduly disrupt or endanger the services to the provider's other customers during an audit or by acknowledging that practical issues such as timing and scope should be discussed in advance. This has been very welcome.

It is also important to note that the EU has introduced into the legislative process a new draft regulatory framework on Digital Operational Resilience for the Financial Sector (DORA) which aims to consolidate and upgrade existing Information and Communications Technology (ICT) risk management requirements, and is also introducing a new direct oversight of critical ICT service providers (including

Google Cloud

cloud service providers) by the European financial regulators. Limited in scope to the provision of technology services to the EU FIs, DORA will nonetheless bring into the regulatory monitoring and oversight global and multinational technology players. This direct oversight framework is meant to set a completely new precedent in regulatory approach to critical outsourcing and third party provider management in the financial services industry in the EU and globally and will - among other things - grant EU supervisory authorities far-reaching investigation and audit powers over third party providers designated as critical to the EU financial services system. Whilst bringing a number or challenges in its current draft, the forthcoming oversight framework for critical third-party providers under DORA could create a genuine opportunity to enhance understanding, transparency, and trust among ICT service providers, financial entities, and financial regulators, and ultimately stimulate innovation in the financial sector in Europe. This approach needs to be further taken into account in the course of the international discussions in due course to understand its benefits and challenges and potential future impact on the global financial services industry and their technology providers. In particular, it will be important to consider how any new regimes sit alongside: (1) existing third party risk management regimes at the country and sector-level, (2) regimes beyond the financial service sector that apply to providers directly at the country-level, and (3) each other at the international-level.

Supply chain and sub-outsourcing risk management

Traditional risk management approaches to supply chain, sub-contractors, and "4th party" risk may not always be compatible when using cloud services because of the inherent multi-tenant nature of those services: one subcontractor will likely service multiple / all customers, meaning that rules that require an individual customer have the right to object to and block the use of specific subcontractors is in many cases logistically and practically infeasible. It is important for the regulators to take into consideration the multi-tenant environment of cloud services when considering sub-outsourcing risk management guidance: any sub-outsourcing criteria needs to be fit-for-purpose for providers' whole customer base whether those entities are regulated or not, and cannot grant one type of customers priority veto rights as such decisions - in particular abrupt termination or change of sub-outsourcers at one customer's demand - could have unintended negative impact on the integrity of the provided services to all customers. Instead, several regulators when specifically considering cloud have encouraged FIs to focus on transparency (including advance notice of new sub-outsourcers) and rigorous due diligence over sub-outsourcers and effective supply chain management by the third party providers.

2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

Third-party dependencies and concentration risk

As a cloud provider, we understand the regulator concerns over perceived market concentration and systemic risk. We agree it is critical to ensure that proper risk mitigants are in place. In our view, **open source and multi-cloud approach** needs to be recognised as part of the solution allowing financial institutions to reduce dependencies and diversify their workloads between different cloud environments.

Google Cloud

Addressing vendor lock-in and concentration risk through the use of multi-cloud approaches is, today, a balancing act between functionality, agility, operational resilience and cost. At one extreme, maintaining parity across two (or more) cloud providers, whilst providing assurance in the event of the failure of one of those providers, is excessively costly and likely to make the firm less competitive and less agile. At the same time, we believe that multi-cloud does have a role to play in addressing this risk, but that it should be done based on an understanding of the criticality of the workloads (and business functions supported), and achieved using open-source based technologies that enable portability at a reasonable cost and within a reasonable timeframe.

Open ecosystems and open source are central to the resilience and open strategic autonomy of cloud services. They provide robust and meaningful mitigations to challenges such as vendor lock-in and "single point of failure" dependencies where critical functions are outsourced to a third party.

We recognise that FIs do not want to be dependent on a single cloud provider to protect sensitive information and deliver critical services. This is an important part of their autonomy and survivability requirements and consistent with the regulators' view on exit strategies. We do not believe it is possible to fully address survivability and substitutability with a proprietary solution. Instead, solutions based on open source and open standards are the route to mitigate the risks and give customers the flexibility to deploy - and, if necessary, migrate - critical workloads across or even off public cloud platforms. This allows use of advanced cloud technologies with the safety net of moving back to on-premises or switching providers and operating without provider assistance if necessary.

An open source approach promotes interoperability and avoids keeping customers tethered to a proprietary technology stack. Google Cloud actively collaborates with the open source community and develops many services on open source technology. We are able to do this by leveraging decades of experience in open source and operating cloud services at scale, including creating and maintaining Kubernetes and Istio.

One of our most important innovations is Anthos, Google Cloud's hybrid- and multi-cloud platform. This is an example of the kind of technology that is central to enhancing resilience. By allowing users to effectively operate their IT stack on any cloud platform including private cloud, resilience and flexibility are boosted, and vendor lock-in can be a thing of the past.

This approach also benefits customers and consumers by offering greater flexibility and provides ecosystem benefits, such as enabling and empowering innovation and workforce development outside Google. It is consistent with our belief that openness enables faster innovation, tighter security, and offers freedom from vendor lock-in.

We recommend for the regulators to consider the following to ensure mitigation of the third party dependencies risks:

Google Cloud

- **Support of a risk and outcome-based approach** to achieve operational resilience and stability objectives;
- Ensure **consistency and coordination of the regulatory approaches** to cloud providers at the global level through principles-based frameworks (including coordination on the impact of the forthcoming regulatory frameworks, such as the UK BoE Operational Resilience Guidance, or the EU Digital Operational Resilience Act);
- **Eliminate fragmentation of regulatory reviews/non-objections for material outsourcing to cloud** and remove - where possible - notification procedures if they act as barriers or duplicative requirements (for example when a provider becomes subject to increased regulatory monitoring and oversight like under DORA the question arises on the potential redundancy of regulatory review for material outsourcing to the said provider);
- **Multi-provider foundation**: no single vendor should have control over the infrastructure. By integrating multiple vendors, lock-in risks and and dependencies on third parties can be reduced. Given the early stage of cloud adoption by many FIs globally, we believe that a multi-cloud strategy needs to remain a business decision based on customer risk assessment instead of a stipulated regulated requirement. However, the regulators need to clearly recognise the benefit of a multi-cloud approach and open source standards and strongly encourage institutions to consider these strategies as part of their cloud migration;
- **Policy endorsement of open source:** real portability and interoperability cannot be fully achieved with proprietary technology and closed ecosystems. Open source is equally important to alleviate concerns over vendor lock-in, dependency on third party providers and address sovereignty and stability needs. Policymakers and financial services regulators need to clearly recognise the benefit of open source standards and containers and strongly encourage their adoption as an industry best practice, and essential provider selection criteria for FIs.
- **A robust interoperability and provider switching ecosystem is critically important for further cloud uptake in the financial services industry.** This will avoid vendor lock-in, diversify available services, and ultimately expand the products offered to the consumers.
- **Application Programming Interfaces (APIs)** allow customers to extract data directly from the cloud providers and do not require temporary storage of data on their local disk.
- Harmonising cloud platforms to allow customers to download their data files in a **common data format**. This makes it easier to import data into new platforms when it is structured in a common format.
- **Data migration features to allow customers to migrate their data from one platform to another**. Providers should use or develop a standardised protocol to support data migration so that data does not get lost during transfer.

Google Cloud

- **International standards as well as exchange of the best practices and information sharing at the global level** is fundamentally important. Regulators should champion adherence to the internationally recognised standards and avoid fragmentation of the standards at the national level. ISO is a good example of a strategic nations collaboration in defining global technical standards under an international umbrella with a solid track record in this space.

Case Study: Solving for Strategic Autonomy on the Cloud

Google Cloud's baseline controls and security features offer strong protections, meet current robust security requirements, and, in most cases, fully address customer needs. This includes critical features such as data residency controls, default encryption for data-at-rest, organisation policy constraints, and VPC Service Controls, among many others. Our whitepaper includes more details on the capabilities that our customers can take advantage of with Google Cloud Platform.

Key to our approach is our commitment to open source-based software solutions that offer control and autonomy, high capability, usability and flexibility, and robust data protection, as well as solutions that expand opportunities to partner with the national cloud service providers and system integrators in the UK to build local skills. Today we have over 500 UK SME partners as part of our Google Cloud partner network, many of which provide services to the government.

To provide even greater security and autonomy for our cloud customers, we are working diligently across three areas:

- ***Data sovereignty** provides customers with a mechanism to prevent the provider from accessing their data, approving access only for specific provider behaviors that customers think are necessary. Examples of customer controls provided by Google Cloud include storing and managing encryption keys outside the cloud, giving customers the power to only grant access to these keys based on detailed access justifications, and protecting data-in-use. With these capabilities, the customer is the ultimate arbiter of access to their data.*
- ***Operational sovereignty** provides customers with assurances that the people working at a cloud provider cannot compromise customer workloads. With these capabilities, the customer benefits from the scale of a multi-tenant environment while preserving control similar to a traditional on-premises environment. Examples of these controls include restricting the deployment of new resources to specific provider regions and limiting support personnel access based on predefined attributes such as citizenship or a particular geographic location.*
- ***Software sovereignty** provides customers with assurances that they can control the availability of their workloads and run them wherever they want, without being dependent on or locked-in to a single cloud provider. This includes the ability to survive events that require them to quickly change where their workloads are deployed and what level of outside connection is allowed. This is only possible when two requirements are met, both of which simplify workload management and mitigate concentration risks: first, when customers have access to platforms that embrace open APIs and services; and second, when*

Google Cloud

customers have access to technologies that support the deployment of applications across many platforms, in a full range of configurations including multi-cloud, hybrid, and on-premises, using orchestration tooling. Examples of these controls are: platforms that allow customers to manage workloads across providers; and orchestration tooling that allows customers to create a single API that can be backed by applications running on different providers, including proprietary cloud-based and open-source alternatives.

Access and audit rights; fourth party risk

As noted above, some of the challenges regarding audits and subcontracting under the existing rules could be alleviated if globally regulators were to follow the approach of those regulators who have acknowledged that - for the security and integrity of all the provider's customers - specific considerations need to apply when dealing with a multi-tenant environment. Allowing these considerations does not inhibit an FI's ability to manage third party risk. Rather it allows risk management practices to continue to evolve to properly apply to new technologies by addressing issues that did not necessarily exist in traditional one-to-one outsourcing arrangements.

3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

The Discussion paper rightfully points out that 'while … understanding the system-wide effects of third-party dependencies is not a new issue, it remains an evolving area for supervisory authorities due to the heterogeneity of services provided and the changing ecosystem'.

We agree that addressing these risks and overall achieving greater operational resilience and stability of the financial system is a collective cross-border challenge. With this in mind, international multi-stakeholder dialogue involving supervisory authorities, firms and third party service providers is essential. Whilst we understand that a certain divergence of views and regulatory practices across different geographies is inevitable and to an extent justified, it is imperative that the regulatory solutions to third party risk management practices across the globe remain proportionate, technologically feasible and consistent in spirit and objectives. The FSB is potentially best placed to facilitate such dialogue and a meaningful exchange of views and best practices, and we would welcome the opportunity to be involved in these discussions as a cloud service provider.

It is important to analyse and accumulate learnings from the existing regulatory practices as well as understand the anticipated impact of the forthcoming policies (such as the EU DORA or the UK Operational Resilience Guidance) to formulate meaningful expectations to an international approach.

Subsequently, we agree with the challenges identified in the Discussion paper that are currently associated with the limitations of regulatory expertise and resources when it comes to monitoring and

Google Cloud

overseeing technology third party providers practices. It is important for this expertise to evolve, and inclusion of the technology providers in the discussions with the regulators is a critical facilitating factor. We would encourage the FSB to convene learning and best practice sharing sessions bringing together all the relevant stakeholders at the global level.

4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

The COVID-19 pandemic has accelerated many trends in technology adoption in the financial services sector, and accentuated the benefits of migration to the cloud to improve financial services institutions' operational resilience and security capabilities. The pace of digital adoption increased in the course of the pandemic in the financial services with consumers shifting to digital banking channels at an unprecedented rate, and capital markets firms having to deal with extraordinary volatility. Many organisations had to move the entire workforce to remote working overnight and shift to primarily digital engagement with their customers. We understand now that this new culture of remote working is not going to go away, and digital technology will continue to underpin day-to-day work practices across many businesses and the public sector, as well as consumer relationships - in particular for financial services.

The pandemic has highlighted the critical need for a holistic crisis response (and more generally, scenarios that require a workforce and customers to be 'dispersed') to be an integral part of FS firms' and their outsourcers' business continuity and operational resilience planning.

What's important to understand is that in the course of the pandemic, cloud providers have continued to demonstrate resilience and enhanced cybersecurity capabilities. At Google Cloud we have not faced nor foresee any shortfalls in our network, compute or customer support capacity. All our technical and personnel readiness steps implemented in response to the pandemic are from our standard playbooks, which were written and have been tested for exactly this type of scenario, well ahead of the crisis. This is strong evidence of how transition to the public cloud can help improve financial services operational resilience - not increase financial stability risks. The geographic scale, redundancy and distribution of our architecture - as well as the principles of openness, portability, and interoperability - are critical to support our customers' resilience and address regulator concerns on the single point of failure.

Modern, digital, cloud-based infrastructure is going to be key to driving ongoing safe and secure innovation and productivity within the financial services sector, for the benefit of consumers and the economy at large. We believe that in the long term the greater risk will come from not moving to cloud and not embracing digital. This is something that the IIF have indicated in their Cloud Computing Paper series[7] first in 2018, and now the COVID-19 industry experience is proving this statement.

[7] https://www.iif.com/Publications/ID/780/PageID/780/IIF-Cloud-Computing-paper-Part-1