Google Cloud

August 22, 2023

Submitted via Email: fsb@fsb.org

The Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: Third-Party Risk Management and Oversight

Google Cloud welcomes the opportunity to provide comments on the Financial Stability Board's (FSB) consultative document entitled "Enhancing Third-Party Risk Management and Oversight" (hereinafter "the Consultation"). As the FSB recognizes, while financial institutions (FIs) have long depended on a variety of third parties in the conduct of their business, they increasingly rely on third-party service providers to provide key benefits such as "flexibility, innovation and improved operational resilience."

Public cloud technology is one third-party service area becoming increasingly important to FIs. Specifically, FIs are increasingly 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, FI have enhanced capabilities to 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 utilize the cloud for a broad range of use cases, including to combat fraud and money laundering through artificial intelligence (AI) and machine learning (ML) models.[1] 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 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 organizations, especially SMEs and smaller firms, can develop on their own. This in turn could lead to protection for investors and financial stability.

At the same time, as adoption has grown, so too have regulatory efforts to understand and address cloud adoption, often resulting in different paradigms and approaches. We believe that clear and

[1] See, as an example, Google AML AI launch (HSBC) in June here.

enabling principles for firms to use cloud services are key to regulators' overall objective to protect investors, ensure market integrity, and maintain financial stability. As such, we applaud the FSB's ongoing efforts "to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and different areas of the financial services sector."

As a provider of cloud services to the financial services industry, Google Cloud works closely with its FI customers to mitigate risks and ensure the seamless provision of cloud services. We believe strongly in supporting the establishment of effective and consistent global regulatory frameworks for such third-party relationships. The Consultation and ongoing work of the FSB are important efforts in this regard. We offer the following comments and feedback to help advance the FSB's work.

I. Recommendations on Key Consultation Topics

A. Common Terms & Definitions (Question 1)

At the outset, Google Cloud strongly supports the FSB's efforts to forge shared understandings of common terms. As the FSB states "[c]ommon understanding of terms and definitions can improve clarity and consistency regarding third-party risk management across financial institutions, assist financial authorities with regulatory cooperation, improve communication with third-party service providers, and promote interoperable approaches that make oversight and risk management more efficient for financial institutions, financial authorities and third-party service providers."

The Consultation proposes a broad definition of a third-party service relationship as "[a] formal arrangement for the provision of one or more services, or parts thereof, to a financial institution by a service provider." While a broad definition may be appropriate for taxonomy purposes, we believe that constraining considerations should come into play in establishing specific risk mitigation expectations for particular third-party service relationships. Otherwise, regulations may establish overbroad expectations that are not appropriately targeted to risk. So, for example, while the Consultation does discuss proportionality as a key principle when considering risk mitigation expectations for particular third-party service relationships, specific and defined standards of "materiality" should be another key principle informing such expectations. More specifically, risk mitigation requirements and expectations should be proportionate to the type, nature, and *materiality* of the service being provided. This same approach should be applied when considering the definition of "outsourcing" in the Consultation, which should similarly be informed by considerations of materiality and proportionality. The FSB's focus on "critical services," as indicated in Section 2.1 of the Consultation, is one example of this kind of tethering of obligations to materiality standards.

B. Proportionality (Question 4)

As noted in the preceding response, Google Cloud believes that the concept of proportionality is critical both in terms of the expectations applied to an FI, in light of its size, sophistication and risks, as well as the expectations applied to a particular service (and provider of that service) in light of its materiality and risks.

As part of the proportionality consideration, regulators should carefully consider the multi-tenant nature of public cloud. Specifically, where financial service regulators address relationships of FIs with third-party providers, measures and obligations can have an impact on other, non-financial customers of the cloud. Disproportionate measures could create risks or disruptions in this service relationship. To avoid this, criteria and parameters should, if and where proposed, be very clear, taking into account the nature of cloud multi-tenancy.

C. *Regulatory Interoperability & Fragmentation (Question 3)*

We appreciate and agree with the FSB's concern with potentially fragmented third-party risk management requirements across global jurisdictions. Consistent standards and expectations across jurisdictions can enhance certainty, reduce wasted spend on idiosyncratic compliance, and result in better and more effective risk management.

Regulatory consistency and coordination within the financial sector and with other authorities that have remit over cloud providers will be essential to make an approach to third-party risk management successful. Where cloud providers are becoming subject to increasing regulatory initiatives in different jurisdictions,[2] regulators should ensure that the exercise of similar powers is based on sound communication and coordination between authorities. We strongly advise against divided sector-specific approaches, since operational resilience and respective risk management needs to be addressed in view of their potential cross-sectoral effects. Consequently, fragmented requirements under different jurisdictions for the same multi-tenant cloud environment would detrimentally impact providers, increase disproportionate workload and costs, and ultimately hamper customers to take up cloud-enabled innovation to the benefit of consumers, industries and public authorities.

We would highlight, in particular, disparate cyber incident reporting requirements across regulators and global jurisdictions as having particularly detrimental effects. Indeed, in our experience, divergent reporting requirements exist even across regulators within national borders. We underscore here that the lack of convergence requires industry actors—FIs and service providers—to spend crucial time and resources navigating regulatory reporting distinctions at the expense of focusing on the primary objective in these cases: detecting, preventing, and mitigating cyber incident risks.

[2] For example in the EU under the Digital Operational Resilience Act (DORA) or in the UK under the supervisory approach to critical third-party providers.

To this end, we encourage the FSB to explicitly recommend that regulators avoid establishing overbroad reporting triggers and explicitly incorporate materiality concepts. The FSB could recommend, for example, that regulators focus reporting obligations on cyber incidents that cause actual material harm or that are reasonably likely to result in actual material harm. We appreciate the FSB's attention to these matters in its Consultation on "CIR Convergence" and rely on our prior comments submitted in response.[3]

D. Contracting (Question 6)

We agree with the FSB that contracts are important tools both for (a) validating the capabilities of a service provider upfront, as well as (b) risk management during the life of the service relationship. We are supportive of efforts by regulators to articulate principles and objectives—as FSB does here—that can help guide contractual arrangements between third-party service providers and FIs, as well as harmonize expectations amongst financial authorities.

These principles and objectives should not, however, be overly prescriptive in setting specific relationship terms, as such approaches will undermine competition by providers to offer enhanced services to customers, result in check-the-box compliance, and box in dynamic and evolving technology-based partnerships. Instead, by communicating principles and objectives without prescribing how they should be achieved, including identified areas of potential risk requiring attention and mitigation, regulators can create a framework for market participants to establish appropriate commercial and contractual terms. These principles and objectives can also help providers and FIs determine and assign appropriate roles and responsibilities in order to most efficiently and effectively satisfy regulatory expectations.

We further support the FSB's position that "the nature and detail of contracts should be appropriate to the financial institution and the criticality of the service." However, as currently drafted, the list in 3.2.2 (Contracting) does not explicitly distinguish between those contract terms that are appropriate for all third-party service relationships and those that are only appropriate for critical services. This could lead FIs and financial authorities to conclude that the FSB's recommendation is that *all* the contract terms listed in 3.2.2 are appropriate for all third-party service relationships. We do not believe this is the intent, especially given how broadly "third-party service relationship" is defined and the burden associated with operationally executing on some of the terms in question. We recommend that the FSB distinguish between contract terms that are appropriate for all third-party service relationships and those that are only appropriate for critical services. In particular, we recommend that the FSB consider limiting the following terms to critical services:

[3] See Google Cloud comments here..

- the financial institution's right to access, audit and obtain relevant information from the service provider, and

- commitments relating to operational resilience, including business continuity, contingency planning and disaster recovery.

Finally, on the topic of contracting, the FSB notes in Section 4.4.2 on cross-border cooperation that financial authorities could see value in the standardization of contract terms. It is unclear whether the FSB is referring to standardization at the country/regional level. If so, we emphasize the challenge that diverging local standard contract terms could pose to service providers who provide services to FIs globally based on common infrastructure and technology.

E. Supply Chain and Sub-Outsourcing Risk Management (Chapter 3.5)

For the reasons the FSB provides, we support the position that "focusing on those nth-party service providers that are knowingly essential to the delivery of critical services to financial institutions or which have access to confidential or sensitive data belonging to the financial institution can be more consistent with a proportionate, risk-based approach".

In addition to the practical limitations the FSB highlights, more traditional risk management approaches to supply chain, sub-contractors, and "nth party" risk may not always be compatible when using cloud services because of the inherent multi-tenant nature of those services: one sub-contractor will likely service multiple or all customers. It is important for regulators to take into consideration the multi-tenant environment of cloud services when considering sub-outsourcing risk management guidance – specifically, any sub-outsourcing criteria needs to be fit-for-purpose for providers' whole customer base whether those entities are regulated or not. As such, certain approaches – for example, an approach that grants one type of customers priority veto rights, such as abrupt termination or change of sub-outsourcers at one customer's demand – would likely have an unintended negative impact on the integrity of the provided services to all customers. Instead, as the FSB recognizes, a better approach is to encourage FIs to focus on transparency (including advance notice of new sub-outsourcers) and due diligence over effective supply chain management by the third party providers.

F. Business Continuity Testing

We recognize that both the FI and the third-party service provider have an important part in achieving adequate business continuity for critical services. However, FIs and service providers would benefit from more clarity on how the requirement to conduct *joint* business continuity testing applies to public cloud - particularly in the context of the shared responsibility model. For example:

FI's role

- FIs can choose to use features or functionality of the cloud service (e.g. multi-regional/zonal architectures, back-up storage) to achieve the desired level of resilience for their critical services. If so, rather than being a reactive action that must be "activated" like a traditional business continuity plan, resilience is inherent based on the way the service is configured and deployed.

- Whatever the level of technical resilience that can be achieved on a cloud service, FIs must plan for the scenario in which the provider can no longer provide the service.

Public cloud provider's role

- Public cloud providers should aim to offer appropriate levels of infrastructure and product availability to enable FIs to deploy their applications in a manner that aligns to their risk appetite and impact tolerances for any critical business processes.

- Public cloud providers should also implement a business continuity plan for the infrastructure, operations and resources required to provide their services.

Both parties should test their own business continuity plans. However, there are constraints and practical limitations on what a public cloud provider can do to support *joint* business continuity plan testing given they provide a multi-tenant service. A public cloud provider can support a FI's business continuity plan testing as follows:

- The provider can supply information and discuss best practices with FIs for using their cloud services to achieve the desired level of resilience or otherwise implement the firm's business continuity plan (e.g best practices for firms seeking to simulate the disruption of services they operate in the cloud).

- If the FI chooses to use cloud service features and availability designs to implement or test the high availability of services, the provider can ensure those features are available and operate as expected during testing.

However, the following types of more direct involvement in testing in an individual FI's business continuity plan testing would be problematic given the nature of public cloud services:

- The provider cannot configure or deploy the cloud services on the FI's behalf to implement or test its business continuity plan. This is entirely within the FI's control. Requiring the provider's involvement is inconsistent with the way cloud services operate.

- The provider cannot simulate a disruption of its service to support a single FI's business continuity plan testing. This could create undue operational risk for the provider's other customers. However, cloud services do enable FIs to simulate a disruption themselves.

In light of this, we suggest that the FSB consider adding a caveat to the requirement to conduct joint business continuity testing with financial institutions (individually or collectively) in 3.6.3 to indicate that this is required "where appropriate to the service being provided."

In addition, we believe that the FSB needs to strongly encourage the authorities to establish effective cross-border cooperation and information sharing and fully support the FSB's call for mutual recognition of testing results and other assurance activities which is essential in the context of multiple new regulatory approaches towards cloud providers that are being developed in parallel across the globe (e.g., EU DORA, UK CTP Policy, EU NISD2 – all of which would introduce new forms of testing and assurances requirements for cloud providers). These forms of mutual recognition would reduce the burden on financial authorities and providers in scope. It would also reduce the risk to the providers' other customers where more disruptive testing tools are used.

Finally, for the reasons above, we also support the FSB's recognition of recognised certifications and standards (e.g. ISO 22301) in the context of public cloud services.

G. Concentration Risk (Question 10)

We agree with the FSB that it is important for FIs to consider potential concentration risks in their relationships with third-parties and we agree it is critical to ensure that proper risk mitigants are in place. In particular, we agree that each FI should only be responsible for assessing concentration-related risks within their institution/group and not for the sector generally. The sector assessment cannot be meaningfully or accurately undertaken by any individual FI as that FI will have no direct or reliable knowledge of if or how any other FI is using a third-party service. Instead, as the FSB recognizes, financial authorities "are best positioned to identify and assess systemic third party dependencies and potential systemic risks."

We also agree with the FSB's position that FIs "can manage concentration and concentration-related risks by deploying the potential tools in the toolkit in a manner commensurate with the overall level of criticality of a concentration." However, we are concerned about the cross-reference to Section 3.5 and the "[c]ontractual rights to assess and consent, or object to the sub-contracting of parts of a critical service that may increase risk" as one such tool for managing concentration risk. Specifically, we understand Section 3.5 to relate to rights to consent to whether or not a provider may sub-contract at all (see e.g., Section 3.5.1, which provides: "[f]or example, contracts between financial institutions and third-party service providers may cover whether the latter may sub-contract critical services (or parts thereof) and, if so, subject to which conditions.") We are concerned that, as

drafted, the cross-reference may be understood as suggesting that FIs should have a contractual right to consent or object to each individual sub-contractor once general approval for sub-contracting has been agreed. Such an interpretation would be impracticable for all of the reasons that that the FSB highlights in Section 3.5.1 and is inconsistent with the focus on information in Section 3.5.2. To reduce the risk of confusion, we suggest a clarification in the text in Section 3.8.3 to ensure that it is more closely aligned with 3.5 and the understanding that the right at issue it to consent (or not consent) to sub-contracting as a whole.

Even as we recognize it is important for FIs to consider potential concentration risks in their relationships with third-parties, however, we do urge consideration of whether and how building such third-party relationships might also improve security and operational resilience as compared to the status quo (which, in the case of cloud services, is usually reliance on an on-premises IT solution). In that regard, a 2021 survey of 1,363 risk/compliance and IT leaders worldwide found that 91% of those surveyed believed that public cloud would enhance operational resilience, 89% believed it would enhance data security capabilities, and 88% were considering implementing a multi-cloud strategy in the near future.[4]

More specifically, with respect to operational resiliency, we underscore that public cloud solutions are definitionally less concentrated and offer greater redundancy and resiliency solutions than traditional on-prem infrastructure. Public cloud providers commonly operate centers across geographic regions in order to diversify capabilities and ensure failover capacity. This architecture is preferable to on-prem solutions that lack similar redundancy benefits.

In our view, considerations of risk of migrating to third-party provided solutions, such as cloud, should take these aspects into account. In addition, an open source and multi-cloud approach needs to be recognised as part of the solution to risks identified by the FSB, allowing financial institutions to reduce dependencies and diversify their workloads between different cloud environments.

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 focused technologies that enable portability at a reasonable cost and within a reasonable timeframe.

[4] Google Cloud/Harris Poll, *The Financial Services Industry Sees Increasing Public Cloud Adoption as Driving Innovation and Compliance* (2021), available at https://services.google.com/fh/files/blogs/report_on_cloud_adoption_in_fsi_google_cloud_08_2021.pdf.

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.

FIs will generally 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 siloed, proprietary solutions—common characteristics of much on-prem architecture. 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. For these reasons, we encourage FSB to consider and acknowledge these technologies and their ability to mitigate the risks identified in the Consultation.

H. "Direct" Incident Reporting (Question 15)

The Consultation asks whether direct reporting by third-parties to regulators in the context of incident notifications should be considered. We respectfully urge the FSB to reject this approach as it would increase confusion across key stakeholders and undermine efforts to promptly resolve such incidents.

As the Consultation notes, current requirements for incident notification to the regulator reside with the regulated FI, not the service provider. The service provider, of course, must work closely with

its FI customer to ensure compliance with notification requirements. This is appropriate for a number of reasons. First, it is the FI (not the provider) that has the relationship with the FI's regulator. Second, and more importantly, in the public cloud context, the service provider is unlikely to be able to determine if an event is notifiable or provide all of the information the regulator will want about the impact of the incident. This is because, to address FI and regulator expectations of security and privacy by design, the cloud service provider does not have visibility or control over the workloads that are deployed by its customers and, therefore, will not know the specific downstream impacts on an incident or be able to explain these to the regulator. In fact, such limited visibility by design is a security and privacy feature that many customers can use to address their regulatory and compliance requirements under existing regulations. The introduction of a direct incident reporting would require operational changes, possibly undercutting established compliance structures for FIs.

Further, if a separate and duplicative requirement to report were imposed on the service provider, added complexity and confusion would be injected into the process. For example, one can imagine the scenario where a single incident results in multiple notifications being made by the regulated FI and the provider to the same regulator—the notifications may not be entirely consistent and could result in confused and/or distracted assessment of the underlying incident, particularly given that the early hours of an incident are often periods in which information is just being gathered and may be thin. Additionally, rather than focusing exclusively on working with the FI customer on the incident, the service provider may end up distracted by its parallel reporting duty to the regulator. This is similar to the challenges that FIs face in the initial hours of an incident due to regulatory fragmentation in incident reporting, as acknowledged in the CIR Recommendations.

Given the service providers' limitations in understanding impact, as well as the significant risk of confusion and diversion of resources given multiple, duplicative reporting lines, we strongly urge the FSB to reject consideration of such additional requirements that would only serve to reduce the effectiveness of incident notification and mitigation efforts at FIs and their service providers.

Extending beyond incident reporting, the FSB notes in Section 4.3.1 that financial authorities in some jurisdictions have acquired direct regulatory powers over financial sector critical service providers, while those in others have not. The FSB then notes that "[t]here is no preference in the toolkit for any particular approach." However, that position does not reconcile with the challenges highlighted in this Consultation and the CIR Recommendations.

First, the CIR Recommendations noted that FIs are subject to multiple reporting requirements for a single incident, not only to multiple financial authorities, but also law enforcement, cyber insurance, industry threat sharing groups etc. Second, as explained in Part C of this submission, sector-specific approaches would almost always result in fragmented requirements, which would detrimentally impact providers, and ultimately hamper FI customers to take up cloud-enabled innovation to the benefit of consumers, industries and public authorities. Consequently, if sectoral regulators,

including financial authorities, were to all acquire direct regulatory powers over their respective sectoral critical service providers, it will almost certainly exacerbate regulatory fragmentation as well as risk duplicative and/or conflicting requirements for the same providers that operate globally at scale as well as service multinational financial institutions. Horizontal technology regulations that apply already to the said critical providers (eg EU NISD2) should also be taken into account by the financial authorities. We therefore urge the FSB to take a stronger stance by discouraging such direct oversight approaches by financial authorities, and to only resort to these only after exhausting other approaches, such as the tools laid out in Chapter 3 of the Consultation.

It might be also useful to consider that several regulators, in the EU, US and UK in particular, have already embarked on a path of direct oversight for critical third party providers albeit through different frameworks. It would be beneficial to allow for this regulatory practice to come into effect and mature for the other regulators to be able to assess its effectiveness and what model could potentially serve as a best practice based on common principled and aligned methodologies across the board.

I. Systemic Risk/Designation of Critical Providers (Question 14)

The FSB properly recognizes that the question of whether an individual institution is overly dependent on a single provider is a distinct question from whether a substantial number of FIs, performing substantially the same activities, are using the same provider in the same jurisdictions, creating a potential for "systemic" risk. The former is properly addressed through existing outsourcing, technology risk management, and/or business continuity regulations, as it should ultimately be the FI that sets its own risk tolerance level and mitigation measures. The latter cannot be mitigated at the institutional level since individual FIs are unlikely to have visibility of other FIs' use of the provider, and equally, service providers may not be able to assess the sector impact given they may only have partial insight into the criticality of the FIs' workloads. This is particularly true of workloads on the cloud. The latter kind of assessment of sectoral or "systemic" risk is best managed by financial regulators playing a sector coordinating and assessment role, challenging firms on their resilience preparations and capabilities, to provide confidence in the entire sector's ability to manage concentration across service providers.

The FSB recognizes that "[c]ritical services are likelier to cause greater and more measurable impacts to financial institutions and, by extension, financial stability if disrupted" while also stating non-critical services may also be relevant. We encourage the FSB to provide more clarity here. In particular, given the focus is systemic risk, "relevance" should be more concretely defined by, or connected to, sector resilience and safety and soundness. Without this clarity, services could be identified as systemic third-party dependencies (and onerous requirements applied) simply because they are provided by a third-party service provider who provides other critical services and not

because they have any genuine impact on systemic risk. In addition, without further clarity, different financial authorities could take different views of the "relevance" of non-critical services.

In the context of cloud, possible measures to address "systemic" risk could include:

- A requirement for financial institutions to maintain and transmit to the regulator a register of the cloud services they are using and what they are using those services for (see e.g., Section 4.3.3 of the Consultation);

- A requirement for the regulator to create a centralized database based on the registered submitted by each financial institution (see e.g., Section 4.3.3 of the Consultation).

These are specifically referenced in the Consultation. In addition, regulators could also consider exploring the following tools:

- Interoperability and portability requirements for financial institutions using cloud services, ideally based on open source technology;

- Resilience and business continuity requirements for financial institutions using cloud services;

- A requirement to consider the appropriateness of a multi-vendor strategy[5].

II. Conclusion

Google Cloud appreciates the opportunity to provide our perspectives on the issues raised in the Consultation. We strongly support the aims of the Consultation to promote proper management and oversight of third-party relationships, reduce fragmentation in regulatory and supervisory approaches across jurisdictions, and facilitate coordination among stakeholders. The FSB stands in a unique position to be able to do so and support the overall dynamism and resilience of the financial services industry globally. We stand ready to provide any further assistance or clarification as needed, and to partner with the FSB and national regulatory authorities to implement the principles and approaches discussed in the Consultation.

[5] For example, see Art. 6 (9) DORA for reference to a multi-vendor strategy by FIs in the EU.