Google Cloud; submitted 8 Oct 2024

Comments on Basel Committee on Banking Supervision ("Committee") Consultative Document - Principles for the sound management of third-party risk" ("Consultation")

Dear Basel Committee on Banking Supervision,

Google Cloud welcomes the opportunity to provide a response to the Committee's Consultation. Public cloud technology is one third-party service area becoming increasingly important to banks. Banks 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 the banking sector. Thanks to the cloud, banks 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. These benefits are fundamental to industry transformation and need to be accounted for in the regulatory guidance.

Banks 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 the banking sector with data protection, data analytics, and operational resiliency capabilities that are more advanced than what individual organizations, especially SMEs and smaller undertakings, can develop on their own. This in turn could lead to greater protection for banking customers 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 enabling principles for banks to use cloud services are key to regulators' overall objective to protect banking customers, ensure market integrity, and maintain financial stability. As such, we applaud the Committee's ongoing efforts to enhance third-party risk management through setting expectations for the adoption of the Principles provided through this Consultation.

As a provider of cloud services to the financial services industry, Google Cloud works closely with its financial institution 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 Committee are important efforts in this regard. We offer the following comments and feedback to help advance the Committee's work:

- **We support the Committee's decision to take a principle-based, proportionate, technology-agnostic approach to third party risk management.**

Google Cloud welcomes the Committee's decision to provide a principle-based, proportionate and technology-agnostic approach towards third-party risk management. The approach taken by the Committee will help banks to reduce third-party risk by focusing on the critical issues that they face rather than follow prescriptive requirements which may not be suited to all types of third-party service provider ("**TPSP**") arrangements.

- **Focusing on the relative benefits (in addition to the costs) of entering into TPSP arrangements is essential to effectively and fairly assessing overall third party risk.**

Google Cloud supports the Committee's decision to include in principle 4 a focus on both the relative benefits and costs, when undertaking due diligence, of new third party services arrangements. As paragraph 38 sets out, it is important to avoid rules and guidance which create obstacles to replacing legacy systems and prevent the adoption of new technologies, which ultimately can cause unnecessary harm to banking customers. The Committee's approach encourages innovation and will be effective in helping banks make informed decisions that ultimately benefit customers and strengthen operational resilience.

- **The definition for and expectations set relating to "nth parties" should include materiality thresholds.**

Google Cloud welcomes the considered approach the Committee has taken to managing risks arising from "nth parties" and its focus on key nth parties. However, to promote a more proportionate and risk-based approach we suggest that the definitions for nth parties and key nth parties be clarified so that they do not extend broadly to all parties who may support the service or critical service delivered to a bank *irrespective* of whether that party's component service part could have a material adverse impact on the security, operational resilience or risk profile more generally of the TPSP's overall service delivery. To achieve this, we suggest that minimum thresholds be included in each definition.

Accordingly, we suggest that paragraph 11 is amended as follows:

• Nth party: A service provider that is part of a TPSP's supply chain and materially supports the ultimate delivery of services to one or more banks. This term includes, but is not limited to, subcontractors of the TPSP.

• Key nth party: A service provider that is part of a TPSP's supply chain and materially supports the ultimate delivery of a critical service by a TPSP to a bank or that has the ability to access sensitive or confidential bank information (eg consumer data).

We also suggest that the considerations for contracts governing TPSP arrangements set out in paragraph 41 not refer to "supply chains" generally, but be limited to "nth parties". Extending the considerations across the supply chain would mean information would need to be provided about a TPSP's entire "network of entities that provide infrastructure, physical goods, services and other inputs" even where those entities do not support the ultimate delivery of services to one or more banks.

We suggest that paragraph 42 be amended as follows:

42. Banks' contracts governing critical TPSP arrangements should at a minimum include the provisions covered in paragraph 41 and those listed below:

• rights for banks to receive accurate, comprehensive and timely information as outlined in the

SLA, including but not limited to information on incidents and material changes to the services of TPSPs or their nth parties~~supply chains~~;.

- **Bank assessments of concentration risk should not need to take into account potentially incomplete information obtained from TPSPs directly regarding their relative systemic importance.**

Concentration risk is a genuine concern that requires continuous monitoring and careful management. It is well supported through reliance on the information banks maintain in their registers which map their third-party dependencies and interconnections. These registers, together with further information obtained through due diligence, provide an accurate source of information against which Banks can conduct assessments of bank-level concentration risk.

We therefore query the expectation for banks to obtain additional information from TPSPs directly to support their understanding of the "relative systemic importance of a TPSP". Bank-level assessments should not be made on the basis of the relative systemic importance of TPSPs but the level of their own exposure to, and reliance upon, each TPSP.

Bank-level concentration risk assessments should also not be based on general, part or incomplete information obtained regarding a TPSP's market presence. Due to confidentiality obligations it will not be possible for TPSPs to reveal details about their service arrangements with other Banks, and in some circumstances, even the existence of those arrangements at all. We therefore request that the expectation that banks obtain information from TPSPs regarding their relative systemic importance be removed and that it be replaced with an expectation that Bank's be informed of a TPSPs relative systemic importance by supervisory authorities where relevant.

We suggest amending paragraph 15 as follows:

"Concentration: Concentration risk[15] in TPSP arrangements may emerge either at the individual bank level or at the systemic level. Monitoring and managing concentration at the individual bank level is the responsibility of the individual bank. While supervisors are best placed to monitor systemic concentrations and inform banks of the relative systemic importance of TPSPs, it is important for banks to understand the ~~relative systemic importance of~~ extent of their reliance on a TPSP, based on available information obtained in mapping their dependencies and interconnections ~~(eg from the public domain, directly from the TPSP)~~, so that they may consider the implications of entering into an arrangement with the TPSP."

Clarity on contractual requirements

- **Allowing for flexibility in choice of governing law can result in more efficient and effective dispute resolution.**

It may not always be the most appropriate or efficient choice for the governing law of the contract to be the law of the jurisdiction where a bank is incorporated or operates for service arrangements with TPSPs. Many TPSPs operate, and provide services to banking groups across multiple jurisdictions, and creating an expectation of preference for the bank's jurisdiction in each and every case could lead to unnecessary complications and inconsistencies in service delivery.

In a banking group context, if subsidiaries were to contract independently with a TPSP and each insist on their own local law, the TPSP could be subject to many different governing laws for providing the same

service across the group, significantly increasing legal complexity for both parties. This could also make service delivery cost prohibitive in some smaller jurisdictions and reduce the ability of small-medium enterprise (SME) TPSPs to enter those markets. Not allowing for flexibility in choice of law could also disincentivise the use of international arbitration and other specialist forums that may be better suited to resolving highly technical or complex financial sector specific disputes, particularly in cross-border contexts, and result in less predictable dispute resolution outcomes.

We suggest amending paragraph 41 as follows:

41. Banks' contracts governing TPSP arrangements should consider:

• choice of law and jurisdiction in case of dispute ~~(where possible, with a preference to apply the laws of the jurisdiction where the bank is incorporated or operating)~~;

- **Some contractual considerations applied to all TPSP arrangements would not be suitable for lower risk contracts.**

Google Cloud welcomes the Committee's statement in paragraph 40 that the details of contracts "should be appropriate to the banks and the criticality of the services provided by the TPSPs." Paragraphs 41 and 42 which follow include two separate lists of contractual considerations for banks, with 41 applying to contracts for all TPSP arrangements and 42 limited to contracts governing critical TPSP arrangements. We suggest clarification that the list of contractual considerations set out for all TPSP arrangements in paragraph 41 be limited to circumstances where those considerations may be relevant to the type of service provided and its risk profile.

For example, as cloud service providers often do not have direct interaction with a bank's retail customers, it would not be appropriate for the contract to address "banking customer complaint handling" by the TPSP. Similarly, neither party would expect to obtain rights to access premises where the bank is receiving a very low risk service which does not have a material operational impact on the delivery of services to banking sector customers. As the Committee has set out in paragraph 15, "certifications and standards can help provide a comparable, baseline level of assurance about TPSPs' controls" for non-critical services (while being supplemented by access and audit rights for critical services).

For non-critical services we suggest that banks should be able to rely on third party audit reports or certifications provided by TPSPs as sufficient alternatives to performing onsite audits. Google Cloud engages independent third party auditors to audit our services based on internationally recognised standards. Our banking customers can review our current certifications and audit reports at any time providing a level of assurance which for some services is proportionate to their criticality and risk profile.

We suggest amending paragraph 41 so that it reads:

> Banks' contracts governing TPSP arrangements should consider (where appropriate):
>
> • rights of banks to ~~access (including premises), audit and~~ obtain relevant information from the TPSPs about the TPSPs' controls, including adherence to certifications and standards,"

We suggest amending paragraph 42 so that it includes the sentence:

> • rights of banks to access (including premises), audit and obtain further relevant information

from the TPSPs;

Paragraph 65 similarly creates an expectation that exit plans for critical services “at a minimum” include various provisions. This statement could be clarified so that it only applies in circumstances where those minimum requirements are relevant.

We suggest amending paragraph 65 so that it reads:

> Banks’ exit plans for the termination of critical TPSP arrangements should, where relevant to the arrangement, at a minimum include the provisions covered in paragraph 64 and those listed below: …

- **Coordination and dialogue amongst supervisors across sectors and borders to monitor systemic risks posed by critical TPSPs for banks is essential.**

Google Cloud strongly supports the Committee's commitment through principle 12 to promoting coordination and dialogue across sectors and borders to monitor systemic risks posed by critical TPSPs for banks. We believe this principle is essential to maintaining stability and resilience as the global financial system becomes more and more digitally interconnected. Many TPSPs, including Google Cloud, provide services to a diverse array of financial institutions which operate across multiple jurisdictions. A coordinated approach to risk monitoring can contribute to a favorable environment for innovation, allowing banks to procure new technology with greater certainty in regulatory compliance. Collaborative efforts can also lead to more efficient and effective risk assessments, benefiting supervisors, TPSPs, banks and ultimately banking customers.

We are grateful for the opportunity to provide comments to the Consultation Document and hope the Committee takes them into consideration. We would be happy to discuss any of our comments in more detail if that would be helpful.

Yours faithfully

Google Cloud