SEBI - Guidelines on Outsourcing of activities by Intermediaries

Google Cloud Mapping

This document is designed to help intermediaries supervised by the Securities and Exchange Board of India (“**regulated entity**”) to consider the Outsourcing of Activities by Intermediaries (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: sections 3 to section 8. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	3 The intermediary shall ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and regulators, nor impede effective supervision by the regulators.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control the Services: ● Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources. ● gcloud Command Tool: A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer’s operating system. ● Google APIs: Application programming interfaces which provide access to GCP. Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Instructions Regulator Information, Audit and Access
2.	3.1 The intermediary shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the service were provided in-house.	This is a customer consideration.	N/A
3.	3.2 Outsourcing arrangements shall not affect the rights of an investor or client against the intermediary in any manner. The intermediary shall be liable to the investors for the loss incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party.	This is a customer consideration.	N/A
4.	3.3 The facilities / premises / data that are involved in carrying out the outsourced activity by the service provider shall be deemed to be those of the registered intermediary. The intermediary itself and Regulator or the persons authorized by it shall have the right to access the same at any point of time.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access Customer Information, Audit and Access
5.	3.4 Outsourcing arrangements shall not impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision/inspection of the intermediary.	Nothing in our contract is intended to limit or impede a regulated entity’s or the supervisory authority’s ability to audit our services effectively.	Enabling Customer Compliance
6.	4 The intermediary shall conduct appropriate due diligence in selecting the third party and in monitoring of its performance.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we’ve provided the information below.	N/A
7.	4.1 It is important that the intermediary exercises due care, skill, and diligence in the selection of the third party to ensure that the third party has the ability and capacity to undertake the provision of the service effectively.	Ability ● Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science,	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. ● Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Capacity ● Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. ● You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard.	
8.	4.2 The due diligence undertaken by an intermediary shall include assessment of:		
9.	a. third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;	Resources and capabilities Information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. Financial soundness You can review Google's audited financial statements on Alphabet's Investor Relations page. Performance The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.	N/A
10.	b. compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;	There are a number of ways to integrate our services with your systems: ● **Cloud Console** allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		- **Cloud APIs** allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.	
11.	c. market feedback of the prospective third party's business reputation and track record of their services rendered in the past;	Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance.	N/A
12.	d. level of concentration of the outsourced arrangements with a single third party; and	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
13.	e. the environment of the foreign country where the third party is located.	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. - Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. - Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		particular: ● The same robust security measures apply to all Google facilities, regardless of country / region. ● Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Location (Service Specific Terms)
14.	5 Outsourcing relationships shall be governed by written contracts / agreements / terms and conditions (as deemed appropriate) {hereinafter referred to as "contract"} that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc.	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract	N/A
15.	5.1 Outsourcing arrangements shall be governed by a clearly defined and legally binding written contract between the intermediary and each of the third parties, the nature and detail of which shall be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the intermediary.	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A
16.	5.2 Care shall be taken to ensure that the outsourcing contract:		
17.	a. clearly defines what activities are going to be outsourced, including appropriate service and performance levels;	Services The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement. Performance levels The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Definitions Services
18.	b. provides for mutual rights, obligations and responsibilities of the intermediary and the third party, including indemnity by the parties;	Responsibilities We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers.	N/A

SEBI - Guidelines on Outsourcing of activities by Intermediaries

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: - Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. - Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers. Indemnity Google provides institutions with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Indemnification
19.	c. provides for the liability of the third party to the intermediary for unsatisfactory performance/other breach of the contract	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Services
20.	d. provides for the continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;	Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: - The **Status Dashboard** provides status information on the Services. - **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services. - **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number	Ongoing Performance Monitoring

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Control You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control the Services: ● Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources. ● gcloud Command Tool: A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer's operating system. ● Google APIs: Application programming interfaces which provide access to GCP.	Instructions
21.	e. includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract shall enable intermediary to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing;	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
22.	f. has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure. Google's confidentiality obligations survive expiry or termination of the contract.	Confidentiality Survival
23.	g. specifies the responsibilities of the third party with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;	IT Security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Insurance Google will maintain insurance cover against a number of identified risks. Business Continuity and Disaster Recovery Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. Force Majeure Refer to your Google Cloud Financial Services Contract.	Insurance Business Continuity and Disaster Recovery Force Majeure
24.	h. provides for preservation of the documents and data by third party;	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Protection of Customer Data Deletion on Termination (Cloud Data Processing Addendum)
25.	i. provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;	Refer to your Google Cloud Financial Services Contract.	Governing Law
26.	j. provides for termination of the contract, termination rights, transfer of information and exit strategies;	Termination rights Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. Regulated entities can elect to terminate our contract for convenience with advance notice if necessary to comply with law and if directed by a supervisory authority. Transfer of information and exit strategies Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to	Term and Termination Transition Term

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: ● **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ● **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. ● You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
27.	k. addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when intermediary outsources its activities to foreign third party. For example, the contract shall include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. These rights apply regardless of the service location. Refer to your Google Cloud Financial Services Contract for more information about the governing law and jurisdiction that applies to our contract	Regulator Information, Audit and Access Customer Information, Audit and Access Governing Law
28.	l. neither prevents nor impedes the intermediary from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and	Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively.	Enabling Customer Compliance
29. I	m. provides for the intermediary and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the third party.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access Customer Information, Audit and Access
30.	6 The intermediary and its third parties shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
31.	6.1 Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines.	Refer to Row 30.	
32.	6.2 An intermediary shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the third party level. Notably,	Refer to Row 30.	

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	it shall consider contingency plans at the third party; co-ordination of contingency plans at both the intermediary and the third party; and contingency plans of the intermediary in the event of non-performance by the third party.	We recognize that, whatever the level of technical resilience that can be achieved on GCP, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: ● Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. ● Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. ● Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)
33.	6.3 To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the intermediary to fulfill its obligations to other market participants/clients/regulators and could undermine the privacy interests of its customers, harm the intermediary's reputation, and may ultimately impact on its overall operational risk profile. Intermediaries shall, therefore, seek to ensure that third party maintains appropriate IT security and robust disaster recovery capabilities.	Refer to Row 23 for information about Google's IT security practices. Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. In addition, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications	N/A
34.	6.4 Periodic tests of the critical security procedures and systems and review of the back-up facilities shall be undertaken by the intermediary to confirm the adequacy of the third party's systems.	You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems)	Customer Penetration Testing Certifications and Audit Reports

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		- ISO/IEC 27017:2015 (Cloud Security) - ISO/IEC 27018:2014 (Cloud Privacy) - PCI DSS - SOC 1 - SOC 2 - SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources	
35.	7 The intermediary shall take appropriate steps to require that third parties protect confidential information of both the intermediary and its customers from intentional or inadvertent disclosure to unauthorised persons.	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Confidentiality
36.	7.1 An intermediary that engages in outsourcing is expected to take appropriate steps to protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. The security of information when using a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: - Our infrastructure security page - Our security whitepaper - Our cloud-native security whitepaper - Our infrastructure security design overview page - Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud	Protection of Customer Data Data Security; Google's Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases ● Security blueprints	
37.	7.2 The intermediary shall prevail upon the third party to ensure that the employees of the third party have limited access to the data handled and only on a "need to know" basis and the third party shall have adequate checks and balances to ensure the same.	Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality.	Data Security; Access and Compliance (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: ● Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). ● Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
38.	7.3 In cases where the third party is providing similar services to multiple entities, the intermediary shall ensure that adequate care is taken by the third party to build safeguards for data security and confidentiality.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
39.	8 Potential risks posed where the outsourced activities of multiple intermediaries are concentrated with a limited number of third parties.	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
40.	In instances, where the third party acts as an outsourcing agent for multiple intermediaries, it is the duty of the third party and the intermediary to ensure that strong safeguards are put in place so that there is no co-mingling of information /documents, records and assets.	Refer to Row 38.	N/A