



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

This document is designed to help the Stock Exchange and clearing corporations supervised by the Securities and Exchange Board of India (“**regulated entity**”) to consider [the Outsourcing of activities by Stock Exchanges and Clearing Corporations](#) (“**framework**”) in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: section 4 (Service Providers/Outsourced agencies and Due Diligence), section 5 (Legal Accountability), section 6 (Sub-contracting), section 7 (Contract with Service Provider/Outsourcing agency), section 8 (Monitoring of Service Provider's/Outsourcing agency's Performance), section 9 (Business Continuity at the Service Provider), section 10 (Security and Confidentiality of Information), section 11 (Termination Procedures), Section 12 (Access to information and other records) and section 13 (Audit). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Workspace services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	4. Selection of Service Providers / Outsourced agencies and Due Diligence	<p>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.</p> <p><u>Ability</u></p> <ul style="list-style-type: none">Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few.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. <p><u>Capacity</u></p> <ul style="list-style-type: none">Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Cloud Customer page.You can review information about Google's historic performance of the services on our Status Dashboard.	N/A
2.	4.1. The service provider / Outsourcing agency shall be subjected to appropriate due diligence to assess its capability to employ a high standard of care in performing the service and comply with its obligations under the outsourcing agreement. The due diligence should take into consideration qualitative and quantitative, financial, operational and reputation factors of the service provider / Outsourcing agency.	See above	N/A
3.	4.2. The exchanges and clearing corporations shall ensure that entities having proven high delivery standards or expertise in the field, are selected after a proper due-diligence process which may include parameters like track record, delivery standard, unique selling proposition, service standards.	See above	N/A
4.	4.3. Due diligence undertaken during the selection process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing.	This is a customer consideration.	N/A
5.	5. Legal Accountability		
6.	5.1. Stock Exchange and clearing corporations shall ensure that there is a legally binding written contract with the service provider / Outsourcing agency.	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
7.	5.2. Stock Exchange and clearing corporation shall ensure that the outsourcing arrangement does not in any way diminish its obligations and those of its board and senior management, to comply with relevant laws and regulations, guidelines and other directions.	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.	Instructions
8.	5.3. The board and senior management of the stock exchange and clearing corporation shall retain ultimate responsibility for the effective management of risks arising from outsourcing.	Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
9.	6. Sub-contracting		
10.	6.1. Stock exchanges and clearing corporations shall ensure that outsourced activities are further outsourced downstream only with the prior consent of the exchange and clearing corporation and with appropriate safeguards including proper legal documentation/ agreement.	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: <ul style="list-style-type: none">• 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 Subcontractors
11.	6.2. Stock exchange and clearing corporations shall also consider the ability of the sub-contractor to perform the services as a part of the due diligence process.	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors
12.	7. Contract with Service Provider / Outsourcing agency		
13.	7.1. Contractual terms and conditions governing relationships, functions, obligations and responsibilities of the contracting parties, potential conflict of interests should be carefully and properly defined in written agreements.	The responsibilities and obligations of the parties are set out in the Google Cloud Financial Services Contract	N/A
14.	7.2. Every outsourcing agreement should address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. Each agreement should allow for renegotiation and renewal to enable the exchange to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
15.	7.3. The agreement should provide for a dispute resolution mechanism, inter-alia specifying the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties in the agreements.	Refer to your Google Cloud Financial Services Contract.	Governing Law; Liability; Indemnification
16.	8. Monitoring of Service Provider's / Outsourcing agency's Performance		
17.	8.1. Stock exchanges and clearing corporations shall maintain the capability and appropriate level of monitoring and control over outsourcing agencies, in order to be able to maintain continuity of business, even in the event of disruption or unexpected termination of the service.	<p><u>Monitoring</u></p> <p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p><u>Control</u></p> <p>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.</p> <p><u>Continuity</u></p> <p>We recognize that, whatever the level of technical resilience that can be achieved on Google Workspace, regulated entities must plan for the scenario in which Google can no longer provide the service.</p> <p>Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page.</p> <p>In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.</p>	<p>Ongoing Performance Monitoring.</p> <p>Instructions</p> <p>Data Export (Cloud Data Processing Addendum)</p>
18.	8.2. Stock exchange and clearing corporation should evaluate its aggregate exposure to a particular service provider / outsourced agency in cases where the institution outsources various functions to the same service provider / outsourced agency.	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 Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.	N/A
19.	8.3. Stock exchange and clearing corporation shall undertake periodic reviews of its outsourcing arrangements to identify new material outsourcing risks as they arise and analyze the impact of the arrangement on its overall risk profile and whether there are adequate internal expertise and resources to mitigate the risks identified.	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation.	N/A



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.</p> <p>Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.</p>	
20.	9. Business Continuity at the Service Provider		
21.	9.1. Stock exchanges and clearing corporations should take appropriate measures to determine that its service providers / Outsourcing agencies establish and maintain emergency procedures and a plan for business continuity / disaster recovery, with periodic testing of backup facilities.	<p>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.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p>	Business Continuity and Disaster Recovery
22.	10. Security and Confidentiality of Information		
23.	10.1. Stock exchanges and clearing corporations should have adequate procedures in place that require the service provider / Outsourcing agency to protect exchange's proprietary, member-related and potentially market sensitive information and software from unauthorized usage.	<p>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.</p> <p>The security of information when using a cloud service consists of two key elements:</p> <p><u>(1) Security of Google's infrastructure</u></p> <p>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p> <p>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.</p> <p>More information is available at:</p> <ul style="list-style-type: none">• Our infrastructure security page• Our security whitepaper• Our cloud-native security whitepaper	<p>Protection of Customer Data</p> <p>Data Security; Google's Security Measures (Cloud Data Processing Addendum)</p>



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">• Our infrastructure security design overview page• Our security resources page <p>In addition, you can review Google's SOC 2 report.</p> <p><u>(2) Security of your data and applications in the cloud</u></p> <p>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.</p> <p><u>(a) Security by default</u></p> <p>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:</p> <ul style="list-style-type: none">• Encryption at rest. Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys.• Encryption in transit. Google encrypts all data while it is "in transit"—traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. <p><u>(b) Security products</u></p> <p>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.</p> <p><u>(c) Security resources</u></p> <p>Google also publishes guidance on:</p>	



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">• Security best practices• Security use cases	
24.	11. Termination Procedures		
25.	11.1. Stock exchanges and clearing corporations should include contractual provisions relating to the termination of the contract and appropriate exit strategies inter-alia specifying events that may trigger termination of the service contract, what will occur on termination and strategies for managing the transfer of the activity back to the stock exchange and clearing corporation or to another party.	<p><u>Termination rights</u></p> <p>Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period.</p> <p>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.</p> <p><u>Transfer and exit strategies</u></p> <p>Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). 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.</p> <p>Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page.</p> <p>In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.</p> <p><u>Deletion</u></p> <p>On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems.</p>	<p>Term and Termination</p> <p>Transition Term</p> <p>Data Export (Cloud Data Processing Addendum)</p> <p>Deletion on Termination (Cloud Data Processing Addendum)</p>
26.	12. Access to Information and other records		
27.	12.1. The outsourcing arrangement should provide for the access by the regulatory authority of the records of service providers / Outsourcing agencies and other information relating to the activities that are relevant to regulatory oversight.	<p>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.</p> <p>Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a</p>	<p>Regulator Information, Audit and Access</p> <p>Customer Information, Audit and Access</p>



SEBI - Outsourcing of activities by Stock Exchanges and Clearing Corporations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none">• ISO/IEC 27001:2013 (Information Security Management Systems)• ISO/IEC 27017:2015 (Cloud Security)• ISO/IEC 27018:2014 (Cloud Privacy)• SOC 1• SOC 2• SOC 3 <p>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.</p>	Certifications and Audit Reports
28.	13. Audit		
29.	13.1. The outsourcing policy document shall act as a reference for audit of the outsourced activities. Audit of implementation of risk assessment and mitigation measures listed in the outsourcing policy document and outsourcing agreement/ service level agreements pertaining to IT systems shall be part of System Audit of Stock Exchanges and Clearing Corporations.	See above	N/A