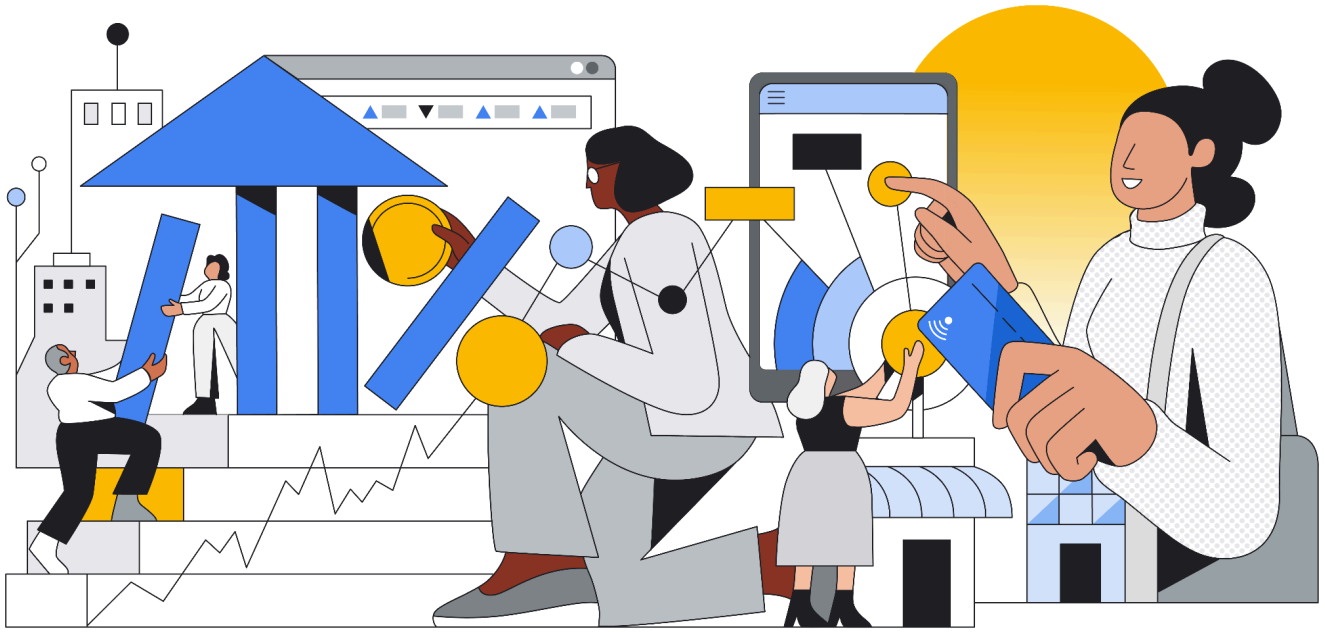
Google Cloud

SEBI Framework for Adoption of Cloud Services: A Guide for Financial Institutions Using Google Cloud in India



Google Cloud

Table of Contents

Disclaimer

This content was last updated in May 2026 and represents the status quo as of the time that it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers. The information in this document is for informational use only, and you are responsible for its assessment. The offerings described are subject to change and do not represent a commitment from Google. All Google Cloud services are provided "as is" and without warranty. This document does not alter the governing legal agreements between you and Google Cloud.

Abstract

India's financial sector is rapidly embracing digital technology, necessitating that SEBI regulated entities keep pace with its ever-changing regulatory landscape.

Leveraging Google Cloud's secure infrastructure and tools can help you meet security and regulatory objectives when designing your cloud environment. This guide is designed to assist institutions regulated by Securities and Exchange Board of India (SEBI), in securely adopting and expanding their use of Google Cloud amidst the evolving digital landscape. This framework will help effectively manage IT risks, enhance cybersecurity, safeguard sensitive data, and ensure operational continuity. Our aim is to expedite your secure adoption of Google Cloud by providing essential information and resources for regulatory compliance. This guide also emphasizes Google Cloud's dedication to security and compliance, outlining how our services align with critical regulatory domains such as IT governance, risk management, cyber defense, data management, and data residency.

This guide includes an in-depth mapping for the below **SEBI Framework for Adoption of Cloud Services by SEBI REs**:

- SEBI Framework for adoption of Cloud Services - 2023

Google Cloud provides the technical capabilities and a shared responsibility model that can help your organization meet these regulatory expectations. The following sections provide more information on how we can support your journey to regulatory compliance.

Google Cloud's Commitment to Security and Compliance

At Google Cloud, we prioritize security and compliance in every aspect of our platform's design and operation. We recognize the critical importance of trust for financial institutions, which is why independent verification of our security, privacy, and compliance controls is a cornerstone of our commitment. Our core strategy involves providing a secure and resilient infrastructure, supported by a comprehensive array of tools and services designed to help you effectively safeguard your data and applications.

Google Cloud ensures compliance by undergoing consistent, independent third-party audits. We are dedicated to upholding vital international standards that establish a strong framework for fulfilling SEBI's compliance requirements. These standards encompass: ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (Cloud Privacy), ISO22301 (Business Continuity Management), PCI DSS, SOC 1, SOC 2, SOC 3, and ISO 42001 (Artificial Intelligence Management Systems).

These certifications affirm our stringent controls concerning information security, cloud-specific security, personal data privacy in the cloud, financial reporting protocols, and AI management systems, thereby providing a reliable foundation for your compliance endeavors. You can

conveniently access Google's current certifications and audit reports on demand through our Compliance Reports Manager, which offers streamlined access to these essential compliance resources.

Enabling Your Compliance

The SEBI guidelines generally place significant emphasis on key aspects of IT governance and IT service provider management, due diligence, risk management and compliance, cyber defense and security, data management and governance, and data residency. Google Cloud offers a comprehensive set of services and features that align with these core domains, enabling you to address the regulations' mandates effectively.

Addressing shared aspects of the regulations

Governance Framework and Accountability

Financial institutions must establish robust cloud governance, ensuring the board and senior management retain ultimate accountability for all outsourced cloud activities and risks. This requires integrating cloud risk management into the existing Technology Risk Management Framework (TRMF) and Cyber Resilience Framework (CRF) of financial institutions. Internal policies must articulate usage criteria commensurate with criticality. The financial institutions must maintain sufficient internal capacity and skilled resources to manage IT outsourcing effectively.

Google Cloud operates on a transparent model where customers retain control over their use of Google Cloud services. You determine which services to utilize, how to configure them, and their specific purpose, ensuring your organization maintains oversight of relevant activities.

- **Control and Management Tools:** You can manage your Google Cloud resources using the Cloud Console (a web-based graphical user interface), the gcloud Command Tool (our primary command-line interface for Google Cloud), and Google APIs (Application Programming Interfaces that provide programmatic access to Google Cloud). These interfaces enable granular control over your cloud environment.
- **Performance Monitoring and Transparency:** You can continuously monitor Google's performance of the services, including adherence to Service Level Agreements (SLAs). The Service Health Dashboard provides real-time status information on Google Cloud services. Personalized Service Health filters disruptive events relevant to your projects, helping you assess impact and maintain business continuity. **Google Cloud Operations** (which includes Cloud Logging, Cloud Monitoring, and Cloud Trace) offers an integrated solution for monitoring, logging, and diagnostics, providing deep insights into your applications running on Google Cloud, including service availability and uptime.
- **Identity and Access Management (IAM):** You can have granular control on end user access permissions, prevent unauthorized actors through Google Cloud's Identity and Access Management controls. Basic, pre-defined and customer roles in IAM help control access for

specific action requirements. Additionally, the IAM Recommender can be used to enforce least-priviledge principles and Privileged Access Management (PAM) can be used to secure sensitive administrative actions.

- **Access Transparency:** This Google Cloud feature provides logs of actions taken by Google personnel concerning your data. Log entries include the affected resource, the time of action, the reason for the action (e.g., the case number associated with a support request), and data about the Google personnel involved (e.g., their location). This offers visibility and auditability into Google's operations, directly supporting your oversight requirements for IT service providers.
- **Access Approval**: This feature 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.

Risk Management and Compliance

The regulations also highlight the increased IT risk exposure for regulated entities, including cyber incidents and data leakage. Google Cloud understands and supports your need to conduct due diligence and perform comprehensive risk assessments before adopting our services.

- **Due Diligence and Third-Party Risk Management (TPRM):** We provide extensive documentation and resources to support your due diligence processes. Google collaborates with independent TPRM providers who conduct regular assessments of Google Cloud's platform and services. These assessments examine security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, and SOC2. The resulting independent audit reports can help streamline and accelerate your internal risk assessment processes. For more information, refer to our Google Cloud Third Party Risk Management Resource Center.
- **Proven Experience and Corporate Information:** With over a decade of providing cloud services, Google Cloud supports customers across diverse sectors globally, including financial services. Our Financial Services Cloud Blog and Financial Services solutions page detail how financial institutions leverage Google Cloud to drive business transformation, foster data-driven innovation, and meet security and compliance objectives. Information about Google's corporate history, mission, business model, strategy, organizational policies (including our Code of Conduct) and audited financial statements are available on Alphabet's Investor Relations page. You can also review information about Google's historical service performance on our Google Cloud Service Health Dashboard.

Cyber Defense and Security

Another significant focus is on strengthening IT organization management to mitigate risks, particularly cyber incidents. Google Cloud provides robust cybersecurity capabilities integrated throughout our infrastructure and services.

- **Security of Google's Infrastructure:** Google manages the security of our infrastructure, encompassing the hardware, software,

networking, and facilities that support the Services. We provide detailed information about our security practices, including our infrastructure security page, security whitepaper, infrastructure security design overview page, and security resources page. To help protect customer data, we run an industry-leading information security operation that combines stringent processes, an expert incident response team, and multi-layered information security and privacy infrastructure.

- **Security of Your Data and Applications:** You are empowered to define the security measures for your data and applications within the cloud. Google proactively takes steps to assist you, including **encryption at rest** (enabled by default with no additional action required from you, as detailed on the Google Cloud Encryption at rest page) and **encryption in transit** (encrypting and authenticating all data when it moves outside physical boundaries not controlled by Google or on behalf of Google, as detailed on the Google Cloud Encryption in transit page). Our SOC 2 report attests to the design and operating effectiveness of controls related to the Trust Services Criteria of security, availability, processing integrity, confidentiality, and privacy. It specifically covers Google's controls that protect customer data on Google Cloud Platform, including logical and physical access, system operations, and change management.

Customer-Configured Cybersecurity and Incident Management (Features in the Cloud)

You define the security measures for your data and applications within the cloud. To enhance your cybersecurity, operational continuity, and incident management capabilities, Google offers a wide range of security products and services for you to configure:

- Operational Resilience & DR Guidance**:** We provide guidance on how you can leverage Google Cloud's inherent reliability features (like zones, regions, and location-scoped resources) and architectural best practices to build robust DR solutions for your cloud infrastructure, as further detailed in our strengthening operational resilience whitepaper.
- Security Command Center (SCC) provides a centralized platform for managing security and risk across your cloud environment. It offers capabilities to prevent, detect, and respond to security issues by integrating services that address vulnerability detection, threat detection, compliance monitoring, and security posture management. SCC helps you gain comprehensive visibility into your assets, identify misconfigurations and threats, and offers tools for effective remediation to strengthen overall cloud security.
- Google Cloud Armor offers robust, global protection against DDoS attacks and provides Web Application Firewall (WAF) services with customizable rules, helping ensure the availability and security of your internet-facing applications.
- reCAPTCHA Enterprise protects websites and applications from fraudulent activity and spam by distinguishing between human users and bots.
- Google Threat Intelligence capabilities leverage Google's vast global network and security expertise to provide customers with continuously updated, actionable insights into emerging threats, enabling proactive defense against sophisticated attacks.
- Google Security Operations unifies security operations with AI-powered analytics to accelerate threat detection, investigation, and response, ultimately strengthening customer security posture.
- Mandiant Cybersecurity Consulting offers strategic services like cyber defense transformation and incident response, enabling customers to proactively enhance their defenses and effectively respond to evolving threats.

- **Operational Resilience:** Google Cloud's disaster recovery (DR) and operational resilience are tightly integrated; DR is a core part of our holistic resilience strategy, ensuring rapid service and data restoration for business continuity. We achieve this through continuous, automated disaster readiness and recovery for all Google's systems and data. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper further elaborates on the importance of resilience, and we also provide guidance on how you can leverage Google Cloud's inherent reliability features (like zones, regions, and location-scoped resources) and architectural best practices to build robust DR solutions for your cloud infrastructure.

Data Management and Governance

The regulations stress the importance of preventing customer personal data leakage and ensuring appropriate data management practices. Google Cloud offers services that facilitate robust data governance, protection, and responsible data processing.

- **Encryption Control and Flexibility:** Encryption is a core component of Google Cloud's security model. While we secure your data at rest and in transit by default, you maintain granular control over your encryption options to meet specific compliance mandates. We offer a comprehensive continuum of key management choices, including those that allow you to generate, store, and rotate your own keys. To align your security goals with the best solution—be it Google-managed keys or customer-managed keys (CMEK) or customer-supplied keys (CSEK)—please refer to our dedicated Choosing an Encryption Option page.
- **Data Access and Use Commitments:** Google commits to accessing or using your data solely to provide the Services you ordered and will not use it for any other Google products, services, or advertising.
- **Subcontractor Compliance:** We require our subcontractors to meet the same high standards, ensuring they comply with our contract with you and only access and use your data as required to perform their subcontracted obligations.
- **Data Protection Laws & Regulations:** Google complies with all national data protection regulations applicable to it in the provision of the Services, as addressed in the Cloud Data Processing Addendum. We are committed to upholding robust data privacy and security measures, including strong contractual commitments, encryption, and transparent practices.
- **Data Loss Prevention: Sensitive Data Protection** helps you discover, classify, and protect sensitive data across your Google Cloud environment, preventing unauthorized access and leakage. It can scan various data sources for sensitive information, such as national identification numbers, credit card numbers, and other personally identifiable information (PII).
- **Secure Data Storage and Analytics: Cloud Storage** provides highly durable, available, and secure object storage for all your data, with options for encryption at rest and in transit. **BigQuery**, our fully managed, petabyte-scale data warehouse, offers robust security features including column-level encryption, row-level security, and auditing capabilities, enabling secure data analytics while maintaining compliance. Services like **Dataproc** allow for secure and compliant processing of large datasets.
- **AI security and privacy:** In deploying AI that addresses both user needs and broader responsibilities, while safeguarding user safety, security, and privacy, Google Cloud has a long-standing commitment to delivering trusted and secure AI, and we incorporate privacy-by-design and default from the beginning. Google Cloud provides clear disclosures and commitments regarding access to a

customer's data. We also enable certain AI/ML services to be configured to meet data residency requirements as noted in our Service Terms. More detail can be found in our Generative AI, privacy and Google Cloud whitepaper.

Data Residency and Cross-Border Transfers

To adhere to the mandates and specific emphasis on data localization for Payment Systems and the processing of IT-Based Transactions, Google Cloud provides choices and controls to help you meet these critical requirements.

- **Region Selection:** Google Cloud offers regions globally, including th**e asia-south1 (Mumbai) and asia-south2 (Delhi)** regions in India. You maintain control over where your data at rest is stored by selecting the specific Google Cloud region or multi-region for your resources, as detailed on our Global Locations page. This capability allows you to deploy your electronic systems and store your data within India, supporting data residency requirements.
- **Data Location and Encryption:** All data stored in Google Cloud is encrypted at rest and in transit. You retain control over your data's location, and our contractual terms specify our commitments regarding data residency and data handling. Using data boundaries, you can configure data residency policies to ensure data remains within designated geographic boundaries, minimizing the need for cross-border transfers where prohibited. More information is available in our Google Cloud Trust Center.
- **Data Incident Response:** Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response process. To assist customers with their own incident response, Google's notification will describe the nature of the data incident, including impacted customer resources; measures Google has taken or plans to take; recommended customer actions; and details of a contact point for more information.
- **Controlled Approach to Government Data Requests:** Google has a rigorous and transparent process for handling government requests for cloud customer data, emphasizing a strong commitment to data protection by carefully evaluating each request, challenging overly broad demands, and providing robust security and privacy controls to customers.

Regulatory Oversight and Contractual Obligations

Outsourcing agreements must contractually grant the financial institution, its external auditors, and the regulator (SEBI) direct, timely, and unrestricted access to all relevant systems, information, and documents to audit and inspect the cloud services used by the regulated entity and access Google's premises used to provide those cloud Services.

Google's contractual commitments in the Cloud Data Processing Addendum apply to all customer data under your account. To enable you to comply with your regulatory oversight requirements and contractual obligations, we provide:

- **Customer's Audit Rights:** Regulated entities always retain the right to conduct an audit. Google offers regulated entities certifications and audit reports in addition to (and not instead of) information, audit and access rights.

- **Supervisory Authorities of Regulated Entities:** 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. 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.
- **Contract Compliance Management:** Google offers specially tailored contractual provisions to regulated entities that help them comply with the contractual requirements under the SEBI regulations. It has provisions including audits, liability for performance, indemnities, business continuity and testing requirements, exit or transition plan. If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.

Compliance with SEBI Framework of Adoption of Cloud

This document is designed to help all regulated entities regulated by the Securities and Exchange Board of India (SEBI) ("regulated entity" , "RE" or "regulated entities") with the information on how Google Cloud supports them with the requirements under the Framework for Adoption of Cloud Services by SEBI Regulated Entities ("framework") in the context of Google Cloud Platform services ("GCP") and the Google Cloud customer agreement. We focus on the following requirements of the framework: Principle 2, 3, 5, 6, 7, 8 and 9 of the abovementioned framework.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	**Principle 2: Selection of Cloud Service Providers**		
2	2) The RE shall ensure that the following conditions are met while choosing any Cloud Service Provider (CSP):		
3	2 (i) The storage/ processing of data (DC, DR, near DR etc.) including logs and any other data pertaining to RE in any form in cloud, should be done within the MeitY empaneled CSPs' data centers holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.	Google Cloud Platform (GCP) services are successfully empanelled by the Ministry of Electronics and Information Technology. The GCP services in the below mentioned link have been STQC audited as per MEITY empanelment process. See here. Listed GCP services has Cloud regions in Mumbai and Delhi NCR which Customers can opt for: Public links:- https://cloud.google.com/about/locations	Data Location (Service Specific Terms)
4	2 (ii) For selection of CSPs offering PaaS and SaaS services in India, the RE shall choose only those CSPs which:	1. Please see row 3 above 2. Please see row 3 above.	

	1. Utilize the underlying infrastructure/ platform of only MeitY empaneled CSPs for providing services to RE. 2. Host the application/ platform/ services (DC, DR, near DR, etc.) provided to the RE as well as store/ process data of the RE, only within the data centers as empaneled by MeitY and holding a valid STQC (or any other equivalent agency appointed by Government of India) audit status. 3. Have a back-to-back, clear and enforceable agreement with their partners/ vendors/ sub-contractors (including those that provide the underlying infrastructure/ platform) for ensuring their compliance with respect to the requirements provided in this framework including those in Principles 6 (Security Controls), 7 (Contractual and Regulatory Obligations) and 8 (BCP, Disaster Recovery & Cyber resilience).	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). Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. Google Cloud also gives you the ability to control the regions where data at rest is stored. In addition, go through our Data boundary via Assured Workloads page. Once the workloads are configured with data boundaries controls, all storage, processing and transit of data is managed within the region of selection. 3. Google is responsible for the performance of all subcontracted obligations. Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Data Location and Assured Workloads Data Location (Service Specific Terms) Google Subcontractors
5	2(iii) Any other additional criteria that the RE considers appropriate/ as per RE's requirement.	This is a customer consideration.	N/A
6	2(iv) The RE shall ensure that storage/processing/ transfer of its data should be done according to requirements provided in this framework as well as any other regulations/ circulars/ guidelines issued by SEBI and any other Government authorities.	Please refer to rows 3 and 4 and customers may assess its requirements.	
7	**Principle 3: Data Ownership and Data Localization**		

8	3(i) Data Ownership: The RE shall retain the complete ownership of all its data and logs, encryption keys, etc. residing in cloud. The CSP shall be working only in a fiduciary capacity. Therefore, the RE, SEBI and any other Government authority authorized under law, shall always have the right to access any or all of the data at any or all point of time.	Google Cloud does not have access to the customer data, unless authorized by the customer. • Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The Google Cloud Trust Center explains how we focus on security, compliance, and privacy to earn the position of your most trusted cloud. With respect to access to data, our contract provides you with the following: • The Customer has access to its data. • Authorized regulators may review information about service operations and controls. • Authorised regulators are granted the right to audit and inspect the services and access Google's premises used to provide those services, subject to reasonable notice and security protocols. Customers can also choose to use External Key management solutions for any additional control on their data. More about External Key management here	Data Security; Additional Security Controls (Cloud Data Processing Addendum) Enabling Customer Compliance
9	3(ii) Visibility: Whenever required (by RE/ SEBI), the CSP shall provide visibility to RE as well as SEBI into CSP's infrastructure and processes, and its compliance to applicable policies and regulations issued by SEBI/ Government of India/ respective state government.	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. As a proactive measure, we have come up with a specially tailed customer agreement to address regulations that apply to financial services customers when they use cloud services. It ensures that regulated entities' use of Google Cloud does not	Enabling Customer Compliance

		increase risk, reduce their control, or hinder their regulator's ability to supervise outsourced activities.	
10	3(iii) Data Localization: In order to ensure that RE and SEBI's right to access RE's data as well as SEBI's rights of search and seizure are not affected by adoption of cloud services, the storage/ processing of data (DC, DR, near DR etc.) including logs and any other data/ information pertaining to RE in any form in cloud shall be done as per the following conditions: 1. The data should reside/be processed within the legal boundaries of India. 2. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data/ transactions/ logs, available and easily accessible in legible and usable form, within the legal boundaries of India. The RE shall ensure that the above-mentioned requirements are fulfilled at all times during adoption/ usage of cloud services.	Refer to row 3 and 4	
11	3(iv) It is to be noted that the REs are ultimately responsible and accountable for security of their data (including logs)/ applications/ services hosted in cloud as well as ensuring compliance with laws, rules, regulations, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, RE shall put in place effective mechanism to continuously monitor the CSP and comply with various regulatory, legal and technical requirements notified by SEBI or any other Government authority from time to time..	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. • 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	Ongoing Performance Monitoring

		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). Incident response Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here. You may also refer to row 19 for additional details on the security measures of Google Cloud.	Significant Developments Data Incidents (Data Processing and Security Terms)
12	**Principle 5: Due Diligence by the RE**		
13	5(i) The REs should evaluate the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing. The RE shall also conduct its due diligence with respect to CSPs beforehand and on a periodic basis to ensure that legal, regulatory, business objectives, etc. of the RE are not hampered. The due diligence shall be risk-based depending on the criticality of the data/services/operations planned to be onboarded on cloud.	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 Cloud Architecture Center helps with reference architectures, design guidance, and best practices for building, migrating, and managing your cloud workloads. In addition, our Security and Reliance framework provides recommendations to ensure continuity and protect businesses against adverse cyber events by using our comprehensive suite of security and resilience solutions. Once on Google Cloud, you can leverage Cyber Insurance Hub to continuously evaluate risk. 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.	N/A

			Also refer to the "Risk Management and Compliance" section of this whitepaper for more details.	
14	5(ii)	A proper due diligence process should be established to assess the capabilities and suitability of a cloud service provider before the engagement.	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. More information on Google Cloud's capabilities is available on our Why 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. 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
15	5(iii)	An analysis (including but not limited to comparative analysis, SWOT analysis, etc.) shall also be conducted on the type of cloud model to be adopted. The analysis should include relevant factors like (including but not limited to) the risks associated with various models, need, suitability, capability of the organization, etc. The above mentioned evaluations/ analyses should be conducted keeping in mind that although the IT services/ functionality can be outsourced (to a CSP), REs are ultimately accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of RE's data and logs, and ensuring RE's compliance with respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same	Please see rows - 13 and 14 - Para 5(i) and 5(ii) above	
16	5(iv)	The criteria that an RE shall look out for are (including but not limited to):		

17	(1)	Financial soundness of CSP and its ability to service commitments even under adverse conditions.	You can review Google's audited financial statements on Alphabet's Investor Relations page. You can also review information about Google's historical service performance on our Google Cloud Service Health Dashboard.	N/A
18	(2)	CSP's capability to identify and segregate RE's data, whenever required	To keep data private and secure, Google logically isolates each customer's data from that of other customers. The Google Security Overview page helps with additional details.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
19	(3)	Security risk assessment of the CSP.	Infrastructure and security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security and confidentiality of 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 • Google Security Overview • 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	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

		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. • Customer Managed Encryption Keys - Customer-managed encryption keys are encryption keys that you own. This capability lets you have greater control over the keys used to encrypt data at rest within supported Google Cloud services, and provides a cryptographic boundary around your data. More information is available on the Google Cloud Customer-Managed Encryption Keys 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: • Explore the Google Cloud Well-Architected framework	

		• Security use cases • Enterprise foundations blueprint Internal control and audit coverage 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) • 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. Reporting Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here. Monitoring	Certifications and Audit Reports Significant Developments Data Incidents (Cloud Data Processing Addendum)

		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 Service Health Dashboard provides status information on the Services. Google Cloud's Observability 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 associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Data back-up Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. Business Continuity Management 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.	Ongoing Performance Monitoring Business Continuity and Disaster Recovery
20	(4) Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership.	Data protection, controls and assurance Refer to Row 19. Access to Data	Enabling Customer Compliance

		You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	
21	(5) CSP's ability to effectively service all the RE's customers while maintaining confidentiality, especially where a CSP has exposure to multiple entities.	Refer Row 19 above. 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)
23	(6) Ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality, SLA, etc	Refer to your Google Cloud Financial Services Contract.	Governing Law
24	(7) RE shall ensure that CSP performs proper screening and background checks of its personnel and vendors before onboarding, and provides adequate trainings and awareness programs to ensure that the customer (RE) services are not hampered due to misconfiguration/inadvertent actions/operational issues/etc.	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 in this document. Refer to our Google Contracting Entity page for information about which Google entity is the provider of the services in each country / region. Each entity is permitted to provide the services in the relevant country / region. Employees Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. Subcontractors 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	N/A Personnel Security - Cloud Data Processing Addendum Google Subcontractors

		confirm that the subcontractor is suitable.	
25	(8) Capability of the CSP to deal with RE's compliance needs, operational aspects, and ensure information security, data privacy, etc	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. As a proactive measure, we have come up with a specially tailed customer agreement to address regulations that apply to financial services customers when they use cloud services. It ensures that regulated entities' use of Google Cloud does not increase risk, reduce their control, or hinder their regulator's ability to supervise outsourced activities. 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) -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 Information on Google's security products is available here which help manage security in the cloud. Here are some examples: • Security Command Center allows you to proactively manage risks and respond to threats with posture management and threat detection for AI, infrastructure, and data. • Web Security Scanner automatically scans App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications for common vulnerabilities.	Enabling Customer Compliance

		• Cloud Security Health Analytics provides visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	
26	(9) CSP's ability to ensure compliance with this framework as well as all applicable rules/ regulations/ circulars issued by SEBI from time to time.	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. As a proactive measure, we have come up with a specially tailored customer agreement to address regulations that apply to financial services customers when they use cloud services. It ensures that regulated entities' use of Google Cloud does not increase risk, reduce their control, or hinder their regulator's ability to supervise outsourced activities.	Enabling Customer Compliance
27	(10) Any other additional criteria that the RE considers appropriate/ as per RE's requirement.	This is a customer consideration	N/A
28	**Principle 6: Security Controls**		
29	6. The RE shall ensure its compliance with the applicable circulars (for example cybersecurity circular, systems audit circular, DR-BCP circular, etc.)/ guidelines/ advisories, etc. issued by SEBI. Further, in reference to the security controls for adoption of cloud computing, the following (including but not limited to) shall be implemented:		
30	6.1(i)1 Vulnerability Management and Patch Management: 1. RE shall ensure that CSP has a vulnerability management process in place to mitigate vulnerabilities in all components of the services that the CSP is responsible for (i.e. managed by the CSP). The RE shall assess and ensure that the patch management of CSP adequately covers the components for which the CSP is responsible (i.e. components managed by the CSP). The patch management framework shall include the timely patching of all components coming under the purview of CSP.	Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

			To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our security whitepaper for more information.	
31	6.1(i)2	The RE shall also ensure that CSP conducts Vulnerability Assessment and Penetration Testing (VAPT) for the components managed by the CSP and fixes the issues/ vulnerabilities within the prescribed timelines (as agreed upon by CSP and RE).	Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. In addition, Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS 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.	Customer Penetration Testing Certifications and Audit Reports
32	6.1(i)3	The RE shall also ensure that the vulnerability management, patch management and VAPT processes are conducted by CSP in-line with the requirements (for example scope, classification of vulnerabilities, duration for closure, etc.) provided in applicable circulars/ guidelines issued by SEBI.	Please refer to our responses in Rows 30 and 31 above. 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

		Additionally, customers can also run penetration tests and report vulnerabilities through the vulnerability rewards program - https://www.google.com/about/appsecurity/reward-program/, which will be acted upon based on severity.	
33	6.1 (ii) Monitoring: RE shall ensure that CSP has adequate security monitoring solutions in place. The monitoring solutions of CSP shall be responsible for the following:		
34	6.1 (ii)1 Monitoring shall cover all components of the cloud. Additionally, the CSP shall continuously monitor the alerts generated and take appropriate actions as per the defined timelines.	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. • 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).	Ongoing Performance Monitoring
35	6.1 (ii)2 The RE shall ensure that any event(s) which may have an impact (financial, reputational, operational, etc.) on the RE shall be intimated to RE by CSP in a timely manner. The reporting should be done in-line with the guidelines/ regulations/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE.	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Significant Developments

		In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here.	Data Incidents (Cloud Data Processing Addendum)
36	6.1 (iii) Incident Management: The RE shall ensure that the CSP has incident management processes in place, to detect, respond and recover from any incident at the earliest. The processes should aim to minimize the impact to the RE.	Please refer to Row 35.	
37	6.1 (iv) Wherever Key management is being done by CSP for platform level encryption (for example, full disk encryption or VM level encryption), RE shall assess and ensure that the entire Key lifecycle management is being done by CSP in a secure manner.	Encryption is a core component of Google Cloud's security model. While we secure your data at rest and in transit by default, you maintain granular control over your encryption options to meet specific compliance mandates. Google performs the entire key lifecycle management when default encryption is used. Google offers a comprehensive continuum of key management choices, including those that allow customers to generate, store, and rotate your own keys. To align to a customer's security goals with the best solution—be it Google-managed keys or customer-managed keys (CMEK) or customer-supplied keys (CSEK)—please refer to our dedicated Choosing an Encryption Option page. provided by Google: • Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. • Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. • Customer-managed encryption keys for Cloud SQL and GKE persistent disks. • Cloud External Key Manager lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure.	N/A

		• Key Access Justification works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.	
38	6.1 (v) Secure User Management: Wherever the user management is done by CSP, the RE shall ensure that role based access and rule based access are strictly followed by CSP for its resources and it shall be based on the principle of least privilege. The following shall also be ensured:	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls. • Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Role Based Access Control (RBAC) helps with basic roles, predefined roles and custom roles to control the set of permissions to perform actions on Google Cloud resources. • Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. • Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. • Privileged Access Management (PAM) can be used to manage just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when. This also helps with time based access control sign temporary access permissions The Google Cloud Trust Center explains how we focus on security, compliance, and privacy to earn the position of your most trusted cloud.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

		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.	
39	6.1 (v)1 Administrators and privileged users shall be given only minimal administrative capabilities for a pre-defined time period, and in response to specific issues/ needs.	See row 38	
40	6.1 (v)2 With respect to administrative privileges/ users, the following shall also be followed: a. All administrative privileges/ users shall be tracked via a ticket/ request by the CSP, and the same shall be provided to the RE on request. Further, the RE shall also track any additional privilege granted to any user by the CSP. b. Access to systems or interfaces that could provide access to the RE's data is granted only if the RE has given explicit time-limited permission for that access.	See row 38	
41	6.1 (v)3 Multi Factor Authentication shall be used for administrator/ privileged accounts.	See row 38	
42	6.1 (v)4 The necessary auditing and monitoring of the above shall be done by CSP and any anomalies shall be reported to the RE	See response for Monitoring and Audit in Row 34 above.	

43	6.1 (vi) Multi-Tenancy: In a multi-tenant cloud architecture, the RE shall ensure that CSP has taken adequate controls to ensure that the RE's data (in transit, at rest and in use) shall be isolated and inaccessible to any other tenants. RE shall appropriately assess and ensure the multi tenancy segregation controls placed by CSP and place additional security controls if required. Any access by other tenants/unauthorized access by CSP's resources to RE's data shall be considered as an incident/breach and the CSP shall ensure that the incident/breach is notified to the RE (as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE, and adequate steps are taken to control the same. During such incident/breach, the RE shall ensure that CSP should provide all related forensic data, reports and event logs as required to the RE /SEBI /CERT-In/ any government agency for further investigation. All conditions and obligations of the RE and CSP under this framework shall also be applicable in multi-tenancy structure.	To keep data private and secure, Google logically isolates each customer's data from that of other customers. It is important for regulated firms 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. Google publishes a number of resources to help customers understand how to configure robust security for our services: • Google Cloud Well-Architected framework • Security use cases • Security foundations blueprints • Security foundation For incident response, please refer to Row 35.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
44	6.1 (vii) The RE shall ensure that the agreement with the CSP contains clause(s) for safe deletion/ erasure of RE's information. The clause should cover various scenarios like business requirement of RE, exit strategy, etc.	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. 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 their own clients. To help regulated entities achieve	Deletion on Termination (Cloud Data Processing Addendum) Transition Term

		this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.	
45	6.1 (viii) For further assurance, the RE may assess the availability of global compliance standards like SOC-2 reporting for CSP.	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) • 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. Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope.	Certifications and Audit Reports
46	6.1 (ix) RE shall ensure that CSP has adequate controls (for example anti-virus, encryption of data, micro-segmentation, etc.) in place to safeguard cloud infrastructure as well as to ensure the privacy, confidentiality, availability, processing integrity and security of the RE's data right from data creation/transfer/etc. In the cloud till final expunging of data.	Please see our response in Row 19 for security controls. Malware Prevention Google's malware prevention strategy begins by preventing infection using manual and automated scanners to scour our search index for websites that might be vehicles for malware or phishing. Every day we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. In addition, we use multiple antivirus engines in Gmail, Google Drive, servers, and workstations to help identify malware. In your Google Cloud environment, you can use Google Security Operations and VirusTotal to monitor and respond to many types of malware.	N/A

		-Google Security Operations helps ingest all your data with twelve months hot data retention and eliminate blind spots with modern threat detection powered by Google. -VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners. Refer to our security whitepaper for more information. Security Monitoring Google's security monitoring program is focused on information that's gathered from internal network traffic, from employee actions on systems, and from outside knowledge of vulnerabilities. A core Google principle is to aggregate and store all security telemetry data in one location for unified security analysis. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. We use a combination of open source and commercial tools to capture and parse traffic so that we can perform this analysis. A proprietary correlation system built on top of our technology also supports this analysis. We supplement network analysis by examining system logs to identify unusual behavior, such as attempts to access customer data. Our security engineers review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis and automated analysis of system logs helps determine when an unknown threat might exist; if the automated processes detect an issue, they escalate it to our security staff. For information about how you can monitor your workloads in Google Cloud, see: • Cloud Monitoring • Security Command Center • Monitoring integrity on Shielded VMs Refer to our security whitepaper for more information.	

47	6.2	Security in the Cloud: RE shall perform risk-based assessment and place adequate controls depending on the criticality of the data/ services/ operations (placed in cloud environment) under the purview of RE. Some of the common controls (including but not limited to) that RE shall put in place are:		
48	6.2.1	Vulnerability Management and Patch Management: The RE shall have a well-defined Vulnerability Management policy in -place and should strictly adhere with the same. The policy should also address the vulnerability management aspects of the infrastructure /services /etc. managed by RE in the cloud. The components managed by RE shall be up to date in terms of patches/OS/version etc. The patch management policy shall also mandate timely patch application.	This is a customer consideration. Google Cloud is responsible for security of the cloud, while the RE should manage the security in the cloud. Refer rows 30, 31 and 32 for understanding more on security of the cloud	
49	6.2.2	Vulnerability Assessment and Penetration Testing (VAPT): The VAPT activity undertaken by RE should cover the infrastructure and applications/services hosted by the RE on cloud. The VAPT tactics, tools and procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system. Additionally, the VAPT activity shall be conducted as per the requirements (including scope, classification, duration for closure of vulnerabilities, etc.) provided in applicable circulars/ regulations issued by SEBI.	Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Customer Penetration Testing

50	6.2.3	Incident Management and SOC Integration: i. The RE shall have incident management policy, procedures and processes in place. The RE shall adhere with the same for deployments being done in cloud. ii. SOC solution (in-house, third-party SOC or a managed SOC) of RE shall be integrated with the services/ application/ infrastructure deployed by RE in cloud. The continuous monitoring shall be done in an integrated manner and the services/ application/ infrastructure deployed in cloud should be treated as an extension of the RE's on premise network. The SOC shall have complete visibility of information systems of the RE deployed on cloud and should be capable to take SOAR actions across the information systems owned by the RE. Additionally, only logs, meta-data should be shipped to shared SOC. REs shall ensure that PII/sensitive data should not be shipped to the SOC.	This is a customer consideration Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here. 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 Service Health Dashboard provides status information on the Services. Google Cloud's Observability 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 associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Data Incidents (Cloud Data Processing Addendum) Ongoing Performance Monitoring
51	6.2.4	Continuous Monitoring: Continuous monitoring shall be done by the RE to review the technical, legal and regulatory compliance of CSP and take corrective measures/ ensure CSP takes corrective measures wherever necessary.	Refer to row 50.	

52	6.2.5 The RE shall ensure that the following Identity, Authentication and Authorization practices are followed (by CSP as well as by RE):		
53	6.2.5 (i) Principle of least privilege shall be adopted for granting access to any resources for normal and admin/privileged accounts.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls. • Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Role Based Access Control (RBAC) helps with basic roles, predefined roles and custom roles to control the set of permissions to perform actions on Google Cloud resources. • Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. • Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. • Privileged Access Management (PAM) can be used to manage just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when. This also helps with time based access control sign temporary access permissions.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)
54	6.2.5 (ii) The identity and access management solution should give the complete view of the access permissions applicable to all resources. The access permissions shall be reviewed regularly in order to remove any unwanted access.		
55	6.2.5(iii) The identity and access management solution should give the complete view of the access permissions applicable to all resources. The access permissions shall be reviewed regularly in order to remove any unwanted access.		
56	6.2.5(iv) Time bound access permissions shall be adopted wherever feasible.		
57	6.2.5(v) Multi factor authentication shall be adopted for admin accounts.		
58	6.2.6(1) Management interface: i. This is the interface provided to the RE by CSP to manage the infrastructure on cloud. This interface is also used to manage the account of the RE assigned by CSP. ii. To mitigate the risks, the interface shall have Two Factor Authentication (2FA)/ Multi Factor Authentication (MFA). For additional security, measures such as dedicated lease lines may be explored. The	Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the following functionality of the Services: • Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources.	Instructions

	access logs and access list to the interface should be strictly monitored (by RE and CSP). The traffic to and from the interface shall be regulated through firewall, Intrusion prevention system, etc.	• 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 will comply with the regulated entity's instructions. Refer to rows 53 to 57 about MFA, identity controls and audit logs.	Scope of Processing; Customer's Instructions (Cloud Data Processing Addendum)
59	6.2.6(2) Internet facing interfaces: Any interface which is exposed to public at large on the internet in the form of a service/API/etc. is considered as internet facing interface. Adequate security controls such as IPS, Firewall, WAF, Anti DDOS, API gateways etc. should be in place and additional controls such as 2FA authentication, SSL VPN solutions shall also be considered.	Google manages the security of our infrastructure, encompassing the hardware, software, networking, and facilities that support the Services. We provide detailed information about our security practices, including our infrastructure security page, security whitepaper, infrastructure security design overview page, and security resources page. Also see rows 53 to 57	N/A
60	6.2.6(2) Interfaces connected between REs/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP: Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. shall be in place and additional controls such as IPSEC VPN shall be adopted, wherever necessary, to secure such interfaces.	See row 59	
61	6.2.7 Secure Software Development: The RE shall undertake Secure Software Development practices for development of cloud-ready applications which shall include (but not limited to): i. RE shall adopt appropriate Secure Software Development processes, and security shall be an integral part right from the design phase itself. ii. A new approach for secure software development shall be implemented by RE for dealing with cloud native development concepts such as micro services, APIs, containers, server less architecture, etc. as the traditional security mechanisms of protecting typical web applications might not be relevant for cloud native development concepts.	This is a customer consideration. Google Cloud has services available for consumption to implement these practices, or a RE can choose to use their own solutions.	N/A

	iii. Best practices such as zero trust principles, fine grained access control mechanism, API Gateways, etc. shall be adopted for development and usage of APIs. End to end security of the APIs shall also be taken care by the RE as per standard practices and guidelines. iv. Secure identification, authentication and authorization mechanisms shall be adopted by the RE.		
62	6.2.8 Managed Service Provider (MSP) & System Integrator (SI): i. Wherever MSP and SI are involved in cloud services procurement, a clear demarcation of roles, and liabilities shall be clearly defined in the Agreement/Contract. ii. As there are new risks introduced in engaging MSP/SI or both, the same shall be assessed, and mitigated by the RE.	This is a customer consideration.	N/A
63	6.2.9(i) To ensure the confidentiality, privacy and integrity of the data, encryption as defined below shall be adopted by the RE: 1. Data-at-rest encryption to be done with strong encryption algorithms. Data object encryption, file level encryption or tokenization in addition to the encryption provided at the platform level shall be used. 2. Data-in-motion including the data within the cloud shall be encrypted. Session encryption or data object encryption in TLS encryption) shall be used wherever any sensitive data is in transit. 3. Data-in-use i.e., wherever data that is being used or processed in the cloud, confidential computing solutions shall be implemented.	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. 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 customer 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. • Customer Managed Encryption Keys. Customer-managed encryption keys are encryption keys that you own. This capability lets you have greater control over the keys used to encrypt data at rest	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

		within supported Google Cloud services, and provides a cryptographic boundary around your data. More information is available on the Google Cloud Customer-Managed Encryption Keys page. • Cloud External Key Manager - A Google Cloud service for using your external keys that are managed within a supported EKM. With Cloud EKM, RE's can use keys that they manage within a supported external key management partner to protect data within Google Cloud. You can protect data at rest in supported CMEK integration services, or by calling the Cloud Key Management Service API directly. 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.	
64	6.2.9(ii) To ensure RE's controls on encryption and Key management, the following shall be followed:		
65	6.2.9(ii)1 Wherever applicable: a. "Bring Your Own Key" (BYOK) approach shall be adopted, which ensures that the RE retains the control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption. b. "Bring Your Own Encryption" (BYOE) approach shall be followed by the RE.	This is a customer consideration. Google Cloud supports customers to bring their own keys using Cloud External Key manager or Customer Managed encryption keys options as detailed in row 63.	N/A
66	6.2.9(ii)2 In case BYOK and BYOE approaches (as given above) are not implemented by RE, the RE shall conduct a detailed risk assessment and implement appropriate risk mitigation measures to achieve equivalent functionality/ security to BYOK and BYOE approaches.	This is a customer consideration	N/A
67	6.2.9(ii)3 Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in a dedicated HSM to have complete control of Key management. However, it is to be noted that HSM should be designed in fault tolerance mode to ensure that the failure of HSM should not have an impact on data retrieval and processing.	This is a customer consideration. Google Cloud supports customers to use their own HSM for key management.	N/A

68	6.2.10 End Point Security:The RE shall ensure that the data security controls in the nature of anti-virus, Data Leak Prevention (DLP) solution etc. are installed and configured on the cloud deployments for effective data security. The RE shall also evaluate the baseline security controls provided by the CSP and may demand additional controls (from CSP) if required.	Malware Prevention Google Cloud's malware prevention strategy begins by preventing infection using manual and automated scanners to scour our search index for websites that might be vehicles for malware or phishing. Every day we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. In addition, we use multiple antivirus engines in Gmail, Google Drive, servers, and workstations to help identify malware. In your Google Cloud environment, you can use Google Security Operations and VirusTotal to monitor and respond to many types of malware. • Google Security Operations helps ingest all your data with twelve months hot data retention and eliminate blind spots with modern threat detection powered by Google. • VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners. Refer to our security whitepaper for more information. Google Cloud has implemented Beyondcorp 100% within the organization and with BeyondCorp Enterprise Integration with Chrome Browser Cloud Management, it enables malware, phishing, and data leakage protection for managed Chrome browsers. Google also has a Data Security Policy, network and computer security policy, reviewed annually which defines how data should be handled at Google to ensure its confidentiality, integrity and availability, and reduces the likelihood of compromise to Google's data and infrastructure from devices connected to Google networks.	N/A
69	6.2.11 Network Security: i. RE shall adopt the micro segmentation principle on cloud infrastructure. Only the essential communication channels	To keep data private and secure, Google logically isolates each customer's data from that of other customers. The Google Security Overview page helps with additional details.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

	between computing resources shall be allowed and the rest of the communication channels shall be blocked. ii. RE shall also consider the option of utilizing Cloud Access Security Broker (CASB)/ Secure Access Service Edge (SASE)/ similar frameworks or tools for effective monitoring of network, enforcement of policies etc.	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. At Google we rely on a zero trust system known as BeyondCorp, to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our What is Zero Trust Identity Security? blog post. Beyondcorp is a mechanism giving results similar to using a CASB or a SASE. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Google's security monitoring program is focused on information that's gathered from internal network traffic, from employee actions on systems, and from outside knowledge of vulnerabilities. A core Google principle is to aggregate and store all security telemetry data in one location for unified security analysis. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. We use a combination of open source and commercial tools to capture and parse traffic so that we can perform this analysis. A proprietary correlation system built on top of our technology also supports this analysis. We supplement network analysis by examining system logs to identify unusual behavior, such as attempts to access customer data. Our security engineers review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis and automated analysis of system logs helps determine when an unknown threat might exist; if the automated processes detect an issue, they escalate it to our security staff.	
70	6.2.12(i) Backup and recovery solution: i. The RE shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud	This is a customer consideration.	

	deployments. The backup and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.	You can use Backup and DR service or Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	
71	6.2.12(ii) The backup shall be logically segregated from production/dev/UAT environment to ensure that the malware infection in such systems does not percolate to backup environment.	This is a customer consideration.	
72	6.2.12(iii) Wherever CSP's backup services are utilized, adequate care should be taken with encryption solution and Key management.	You can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	Business Continuity and Disaster Recovery
73	6.2.13 RE shall equip staff overseeing cloud operations with the knowledge and skills required to securely use and manage the risks associated with cloud computing. The skills should also be imparted to oversee the management interfaces, security configurations etc. of CSP infrastructure. This is a critical factor as it will reduce the misconfigurations, vulnerabilities etc. and will increase the reliability of services.	This is a customer consideration. The responsibility to meet this requirement for its staff is with the customer. Google provides the following tools and information to the customer: • Google provides the Cloud Console and Admin Console, which allow your staff to manage security configurations and monitor services. • Google makes available Security Documentation, including security whitepapers to use the Services securely. • Google ensures that its own personnel are trained in security and privacy as detailed in the Cloud Data Processing Addendum (CDPA).	N/A
74	6.2.14 CSP shall notify the RE of any cybersecurity incident (for example data breach, ransomware, etc.) as mandated by the RE. The reporting shall be done as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE. The CSP shall provide all related forensic data, reports and event logs as required by RE/ SEBI/ CERT-In/ any other	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in	Significant Developments

	government agency. The incident shall be dealt as per the Security Incident Management Policy of the RE along with the relevant guidelines/ directions issued by SEBI/Government of India/ respective state government.	accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here and under the Data Incidents section of the CDPA.	Data Incidents (CDPA)
75	**Principal 7: Contractual and Regulatory Obligations**		
76	7(i) A clear and enforceable cloud service provider engagement agreement should be in place to protect RE's interests, risk management needs, and ability to comply with supervisory expectations.	The terms and conditions governing the relationship between the parties are set out in the Google Cloud Financial Services Contract. 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.	
77	7(ii) The contractual/agreement terms between RE and CSP shall include the provisions for audit, and information access rights to the RE as well as SEBI for the purpose of performing due diligence and carrying out supervisory reviews. RE shall also ensure that its ability to manage risks, provide supervision and comply with regulatory requirements is not hampered by the contractual terms and agreement with CSP.	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. 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. Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the following functionality of 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.	Enabling Customer Compliance Instructions Scope of Processing; Customer's Instructions (Cloud Data Processing Addendum)
78	7(iii) The contract/agreement shall be vetted with respect to legal and technical standpoint by the RE. The agreement shall be flexible enough to allow the RE to retain adequate control over the resources which are on boarded on cloud.The agreement should also provide RE the right to intervene with appropriate measures to meet legal and regulatory obligations.		

		Google will comply with the regulated entity's instructions unless prohibited by applicable law. Ongoing Monitoring and Visibility: To ensure effective monitoring, Google provides a suite of monitoring tools. Please refer to row 88.	
79	7(iv) SEBI/ CERT-In/ any other government agency shall at any time: 1. Conduct direct audits and inspection of resources of CSP (and its sub-contractors/ vendors) pertaining to the RE or engage third party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ circulars and standard industry policies. 2. Perform search and seizure of CSP's resources storing/ processing data and other relevant resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency may access RE's IT infrastructure, applications, data,documents, and other necessary information given to, stored or processed by the CSP and/ or its sub-contractors. 3. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents) related to RE. 4. Seek the audit reports of the audits conducted by CSP. The RE shall ensure that adequate provisions are included in the agreement/ contract with CSP to enable the above functionalities. Additionally, RE shall also include provisions (in the contract/ agreement with CSP) mandating that CSP extends full cooperation to SEBI while conducting the above-mentioned activities.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, discussion about the services with Google personnel (including subject matter experts), audit and access rights to regulated entities, supervisory authorities, and both their appointees. In addition, Customer will at all times have access to customer data (including customer's virtual machines and customer applications) using the standard functionality of the Services and may provide access to the Regulator at Customer's discretion. With respect to data incidents, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. With respect to CSP's audit reports, please refer to row 80(3)	Enabling Customer Compliance Regulator Information, Audit and Access Data Incidents (Cloud Data Processing Addendum)

80	7(v) The RE shall also ensure that adequate provisions are included in the agreement/ contract for the following audit/ VAPT functions: 1. CSP shall be responsible for conducting audit/ VAPT of the services/ components managed by the CSP. 2. The RE shall be responsible for conducting audit/ VAPT of the services/ components managed by the RE. The audit/ VAPT shall be conducted as per the requirements (including scope, duration for closure of vulnerabilities, etc.) provided in various applicable circulars/ regulations issued by SEBI from time to time. 3. Implementation and configuration audit of the resources to be deployed by the RE in cloud environment shall be conducted by the RE and the same shall be certified by the RE after closing all non-compliances/ observations before go-live. 4. The RE may take into consideration the report/certificate of the audit of the CSP conducted by STQC. However, wherever required, CSP has to conduct additional audits (from CERT-In empaneled auditors) to fulfil all the requirements provided in various applicable circulars/ regulations issued by SEBI, and the same shall be ensured by the RE. 5. The RE shall ensure that appropriate clauses/ terms (including SLA clauses) are added in the agreement (signed between RE and CSP) to enforce the above-mentioned audit/ VAPT requirements.	1. Please refer to our responses in Rows 30 and 31 above. 2. Please refer to our responses in Rows 30 and 31 above. 3. 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) • 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. 4. Google Cloud Platform (GCP) services are successfully empanelled by the Ministry of Electronics and Information Technology. The GCP services have been STQC audited as per MEITY empanelment process. See here. Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. In addition, Google also grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. 5. Service Levels. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is	Enabling Customer Compliance, Regulator Information, Audit and Access

		available at our Incidents & the Google Cloud dashboard page.	
81	7(vi) Contract/Agreement should have adequate provisions regarding the termination of contract with CSP, and appropriate exit strategies to ensure smooth exit without hindering any legal, regulatory or technical obligations of the RE.	Transition: Regulated entities can terminate our contract with advance notice. 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 their own clients. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google can provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services. Exit strategy: Google Cloud offers the flexibility to migrate, build, and optimize apps across hybrid and multicloud environments. Google is one of the largest contributors to the open source ecosystem. We work with the open source community to develop well known open source technologies like Kubernetes, then roll these out as managed services to give users maximum choice. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Google recognizes 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 Portability: Through Google Cloud Data Portability and Switching Procedures, our platform provides transparent and flexible methods for managing and moving data.	Term and Termination Transition Term Transition Assistance Data Export (Cloud Data Processing Addendum)

		• Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by on-premise. • Google's approach to sovereign cloud solutions - Google Distributed Cloud is a portfolio of hardware and software solutions that helps extend Google Cloud infrastructure to the edge and into your data centers. Google recognizes the importance of continuity for regulated firms and for this reason we are committed to data portability and open-source. Refer, Data Transfer Essentials which offers a cost-effective way to move data between the services of an application that resides across multiple CSPs, while adhering to regulatory requirements.	
82	7(vii) As part of exit strategy, a clear expunging clause shall be defined in agreement with CSP, which shall state that whenever the RE intends to expunge the data, CSP shall securely and permanently erase the RE's data in disks, backup devices, logs, etc. and no data shall remain in recoverable form. However, it is the responsibility of the RE to ensure that the minimum retention requirements for data (including logs) as prescribed by SEBI/ Government of India/ respective state government are met and that the required data, logs, etc. are archived, even if the RE moves out of the cloud/ changes CSPs.	Destruction of data 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.	Deletion on Termination (Cloud Data Processing Addendum)
83	7(viii) The RE shall ensure that their data (including but not limited to logs, business data, etc.) is stored in an easily accessible, legible and usable manner (during utilization of cloud services and after exit from the cloud) and it shall be provided to SEBI/ any other government agency whenever required.	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. In addition, customers will at all times have access to customer data (including customer's virtual machines and customer applications) using the standard functionality of the Services and may provide access to the Regulator at Customer's discretion.	Enabling Customer Compliance Regulator Information, Audit and Access Customer Information, Audit and Access
84	7(ix) The RE is required to adhere with SEBI circulars/guidelines issued from time to time and the cloud framework shall be seen as an addition/ complementary to existing circulars/ guidelines and not as a replacement.	This is a customer consideration	N/A

85	7(x) The agreement/contract made by RE shall also include (but not limited to) below mentioned terms/ provisions/ clauses:		
86	7(x)1 Definition of the IT activities and resources being on boarded on cloud, including appropriate service and performance standards including for the material sub-contractors, if any.	Services The GCP services are described here. Service Levels The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. Subcontractors Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you	Definitions Services Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum) Google Subcontractors
87	7(x)2 Effective access to all the objects/ information relevant to the RE/ RE's operation including data, books, records, logs, alerts, and data centre.	Google recognizes that regulated entities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Customer Information, Audit and Access
88	7(x)3 Continuous monitoring and assessment of the CSP by the RE so that any necessary corrective measure can be taken immediately, including termination of contract and any minimum period required to execute such provisions, if deemed necessary.	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.	Ongoing Performance Monitoring

		• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • 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).	
89	7(x)4 Type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the RE to take prompt mitigation and recovery measures and ensure compliance with statutory and regulatory guidelines.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here.	Significant Developments Data Incidents (Data Processing and Security Terms)
90	7(x)5 Compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer (RE) data.	Google will comply with all laws, regulations and binding regulatory guidance applicable to Google in the provision of the Services.	Representations and Warranties
91	7(x)6 The deliverables, including SLAs, for formalizing the performance criteria to measure the quality and quantity of service levels.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
92	7(x)7 Storage of data (as applicable to the RE) within the legal boundaries of India as per extant regulatory requirements.	Please refer to row 3	
93	7(x)8 Clauses requiring the CSP to provide details of data (captured, processed and stored) related to RE and RE's customers to SEBI/ any other government agency.	The regulated entity will at all times have access to their data (including its virtual machines and customer applications) using the standard functionality of the Services and regulated entity may provide access to the regulator at their discretion.	Enabling Customer Compliance
94	7(x)9 Controls for maintaining confidentiality of data of RE and its customers, and incorporating CSP's liability to the RE	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	Confidentiality

	in the event of security breach and leakage of such information.	contract and to protect that information from disclosure. This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 19 for more information about the security of our services.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
95	7(x)10 Types of data/ information that the CSP is permitted to share with the RE's customers and/or any other party.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account.	N/A
96	7(x)11 Specifying the resolution process for events of default, insolvency, etc. and indemnities, remedies, and recourse available to the respective parties.	If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Refer to your Google Cloud Financial Services Contract for more information indemnities, remedies and recourse available to our customers In addition, regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution. Upon request, Google can provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Term and Termination Support through Resolution Transition Term
97	7(x)12 Contingency plan(s) to ensure business continuity planning, RPO/RTO, and recovery requirements.	Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including: • destruction of infrastructure required to provide the Services • interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures) • unavailability of key personnel	Business Continuity and Disaster Recovery.

		• emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) • pandemics 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.	
98	7(x)13 Provisions to fulfill the search and seizure requirements (as provided above in this principle) and audit/ VAPT requirements (as provided above in this principle).	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. The regulated entity is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit regulated entities to a fixed number of audits or a pre-defined scope. For more details on VAPT, see rows 30, 31 and 32	Enable Customer Compliance, Customer Information, Audit and Access.
99	7(x)14 Right to seek information (by RE/ SEBI) from the CSP about the third parties (in the supply chain) engaged by the CSP.	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services they 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 will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors

100	7(x)15 Clauses making the CSP contractually liable for the performance and risk management practices of its sub-contractors.	Refer row 99	
101	7(x)16 Obligation of the CSP to comply with directions issued by SEBI in relation to the activities of the RE on boarded on cloud.	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. This includes access to Google's premises used to provide the Services to conduct an on-site audit. In addition, the customer will at all times have access to customer data (including customer's virtual machines and customer applications) using the standard functionality of the Services and customer may provide access to the regulator at its discretion.	Enabling Customer Compliance
102	7(x)17 Termination rights of the RE, including the ability to orderly transfer the proposed cloud onboarding assignment to another CSP, if necessary or desirable.	Regulated entities can terminate our contract with advance notice. 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 their own clients. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google can provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Term and Termination Transition Term Transition Assistance
103	7(x)18 Obligation of the CSP to co-operate with the relevant authorities in cases involving the RE as and when required.	Google recognizes that regulated entity customers are subject to the supervision of a regulator and requires 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 including fully cooperating with the regulator during conduct of audits, inspection of services and access to Google's premises used by Google to provide the services to the regulated entities, subject to reasonable notice and security protocols.	Enabling Customer Compliance
104	7(x)19 Clauses for performing risk assessment by CSP with respect to hiring of third party vendors, the checks/	Refer row 99	

	process followed by CSP before onboarding personnel/ vendors, etc.		
105	7(x)20 Any other provision(s) required to ensure compliance with respect to circulars/ guidelines/ regulations (including this cloud framework) issued by SEBI.	Refer to your Google Cloud Financial Services Contract. The Google Cloud Financial Services Contract is specifically tailored to provide financial services customers globally to address the contract language they need to address their regulatory requirements.	N/A
106	7(xi) Wherever the System integrator or managed service provider or both, along with CSP are involved, the contractual terms and agreement shall unambiguously demarcate/ delineate the roles, and liabilities of each participating party	The terms and conditions governing the relationship between the RE and Google Cloud are set out in the Google Cloud Financial Services Contract. 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. It is important for customers 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. More on Shared responsibility - here It is also the customer's consideration in engaging a system integrator or a managed service provider or both, and Google will not be involved in that agreement and transaction.	
107	7(xii) If any function/ task/ activity has to be performed jointly by the RE and CSP/MSP/SI, there shall be a clear	Refer to row 106	

	delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP (and MSP/SI wherever applicable). However, any such clause in the agreement shall not absolve the RE from having the ultimate responsibility and liability for any violation of the laws, rules, regulations, circulars, etc. issued by SEBI or any other authority under any law, regardless of any delineation/ demarcation of responsibilities.		
108	7(xiii) Similarly, there shall be an explicit and unambiguous delineation/ demarcation of responsibilities between the RE and CSP (and MSP/SI wherever applicable) for ensuring compliance with respect to applicable circulars (for example cybersecurity and cyber resilience circular, outsourcing circular, BCP-DR etc.) issued by SEBI from time to time. There shall be no "joint/ shared ownership" for ensuring compliance with respect to any clause. If compliance for any clause has to be jointly ensured by RE and CSP (and MSP/SI wherever applicable), there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the clause. This delineation shall also be added explicitly in the agreement (as an annexure) signed between the RE and the CSP.	Refer to row 106	
109	7(xiv) Reporting Requirements: 1. It is being reiterated that the RE is solely accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. 2. The RE shall explicitly and unambiguously specify the party (RE or CSP/MSP/SI) which is responsible for ensuring compliance with each clause of the applicable SEBI circulars (for example cybersecurity circular, systems audit, etc.) in its audit reports.	This is a customer consideration	N/A

	There shall be no "joint/ shared ownership" for any of the clauses. In case the responsibility of ensuring compliance (for any clause) rests with both parties, the task shall be split into sub-tasks/line-items, and for each sub-task/line-items, the responsible party shall be indicated in the report. 3. The RE shall ensure that the demarcation/ delineation of responsibilities is provided for each clause of the applicable SEBI circular(s). 4. In view of the above requirements, as well as to ensure effective monitoring of cloud deployments by REs, reporting of compliance (with this framework) shall be done by the REs in their systems audit, cybersecurity audit and VAPT reports, and it shall be done in the standardized format notified by SEBI from time to time. 5. Reporting by Auditor: As part of system audit of the RE, the auditor shall verify, and certify, whether there is a clear delineation/ demarcation of roles and responsibilities between the RE and CSP/MSP/SI (in-line with the "Principle 4: Responsibility of the RE" of the framework): a. For each task/ function/ activity/ component (including the tasks/ functions stated in clause (x) above, wherever applicable). b. For each clause of applicable/ relevant SEBI circular/ guidelines/ regulations. The auditor shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and CSP (and MSP/SI wherever applicable).		
110	7(xv) In the event of any CSP deployed by an RE losing its empanelment status with MeitY/ commits a passive breach of contract/ agreement in any way, the RE shall ensure that it becomes compliant with this framework within 6 (six) months of being notified of/ discovering the breach.	This is a customer consideration.	N/A
111	**Principle 8: BCP, Disaster Recovery & Cyber Resilience**		

112	8(i) The RE shall assess its BCP framework and ensure that it is in compliance with this cloud framework as well as other guidelines/ circulars issued by SEBI from time to time.	This is a customer consideration. 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 contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
113	8(ii) RE shall also assess the capabilities, preparedness and readiness with respect to cyber resilience of CSP. The same can be periodically assessed by conducting DR drills (in accordance with circulars/ guidelines issued by SEBI) by involving necessary stakeholders.	Refer to row 112	
114	8(iii) Additionally, RE shall develop a viable and effective contingency plan to cope with situations involving a disruption/ shutdown of cloud services.	This is a customer consideration.	N/A
115	**Principle 9: Vendor Lock-In and Concentration Risk Management**		
116	9(i) RE shall assess its exposure to CSP lock-in and concentration risks. The risk evaluation shall be done before entering into contract/ agreement with CSP and the same should also be assessed on a periodic basis.	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 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 Google Distributed Cloud(GDC) which is a portfolio of hardware and software solutions that provides an option to extend Google Cloud infrastructure to the edge and into your own data centers to build, deploy and optimize your applications in both cloud and on-premises environments. To understand the different components of GDC, see here.	Data Export (Cloud Data Processing Addendum)
117	9(ii) In order to mitigate the CSP concentration risks, RE shall explore the option of cloud-ready and CSP agnostic solutions (such as implementing multi-cloud ready solutions) which can facilitate the RE in migrating the solutions as and when necessary, with minimal changes. Exit strategies shall be developed, which should	Google recognizes the importance of continuity for regulated firms and for this reason we are committed to data portability and open-source. Refer Google Cloud Data Portability and Switching Procedures to understand more on transparent and flexible methods for managing and moving data, and also Data	Data Export (Cloud Data Processing Addendum)

	consider the pertinent risk indicators, exit triggers, exit scenarios, possible migration options, etc.	Transfer Essentials which offers a cost-effective way to move data between the services of an application that resides across multiple CSPs, while adhering to regulatory requirements. To manage concentration risk, you can choose to use Google Distributed Cloud(GDC) which is a portfolio of hardware and software solutions that provides an option to extend Google Cloud infrastructure to the edge and into your own data centers.to build, deploy and optimize your applications in both cloud and on-premises environments. To understand the different components of GDC, see here. In addition, 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. • Google Distributed Cloud allows you to create GKE clusters in your own on-premises data center (on your hardware or in a VMware environment). • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. 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. Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business,	Deletion on Termination (Cloud Data Processing Addendum) Transition Term

		without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to 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.	
118	9(iii) The RE shall also take measures to implement data portability and interoperability as part of exit/ transfer strategy.	Refer row 117	
119	9(iv) In order to mitigate the risk arising due to failure/ shutdown of a particular CSP, and to limit the impact of any such failure/ shutdown on the securities market, SEBI may specify concentration limits on CSPs (thereby setting a limit on the number of REs that a CSP may provide its services to).	Refer row 117	

Shared Responsibility and Shared Fate on Google Cloud

Operating in the cloud involves a shared responsibility model, where Google Cloud and our customers both play essential roles in ensuring security and compliance. Google is responsible for the security *of* the cloud, meaning we secure the underlying infrastructure, network, and foundational services that support your operations. This includes our global data centers, hardware, software, networking, and the processes and controls for maintaining these systems.

Conversely, you, the customer, are responsible for security *in* the cloud. This entails the security of your configurations within the cloud environment, the security of your applications and data, identity and access management, network configurations, and the overall security posture of your cloud deployments. Our shared fate model signifies that we succeed together; your compliance is a collective objective, and we provide the platform and tools to assist you in achieving it. While Google Cloud furnishes a secure platform and comprehensive tools, the ultimate responsibility for achieving and maintaining compliance with the laws and regulations rests with your organization, based on your specific implementation and operational practices. For more details on this model, refer to the Shared Responsibility and Shared Fate documentation.

Partnering on Your Compliance Journey

Google Cloud

Google Cloud is more than a technology provider; we are your partner in navigating the complexities of regulatory compliance. We are dedicated to continuously enhancing our platform and services to help financial institutions in India meet evolving requirements and innovate securely.

We encourage you to explore Google Cloud's comprehensive compliance resource center to access whitepapers, compliance guides, and detailed documentation relevant to the financial sector and data governance, including the Google Cloud Trust Center, Security section, Geography and Regions documentation, Security Best Practices, and Privacy information. To accelerate your deployment, you can also leverage our pre-built resources like the Google Cloud Security Foundations Blueprint as a starting point.

For guidance on how Google Cloud can support your journey to comply with specific SEBI regulations, please do not hesitate to contact your Google Cloud account team. We are here to help you build and operate secure, compliant, and transformative solutions in the cloud.