Google Cloud

Reserve Bank of India (Commercial Banks – Managing Risks in Outsourcing) Directions, 2025: A Guide for Financial Institutions Using Google Cloud in India

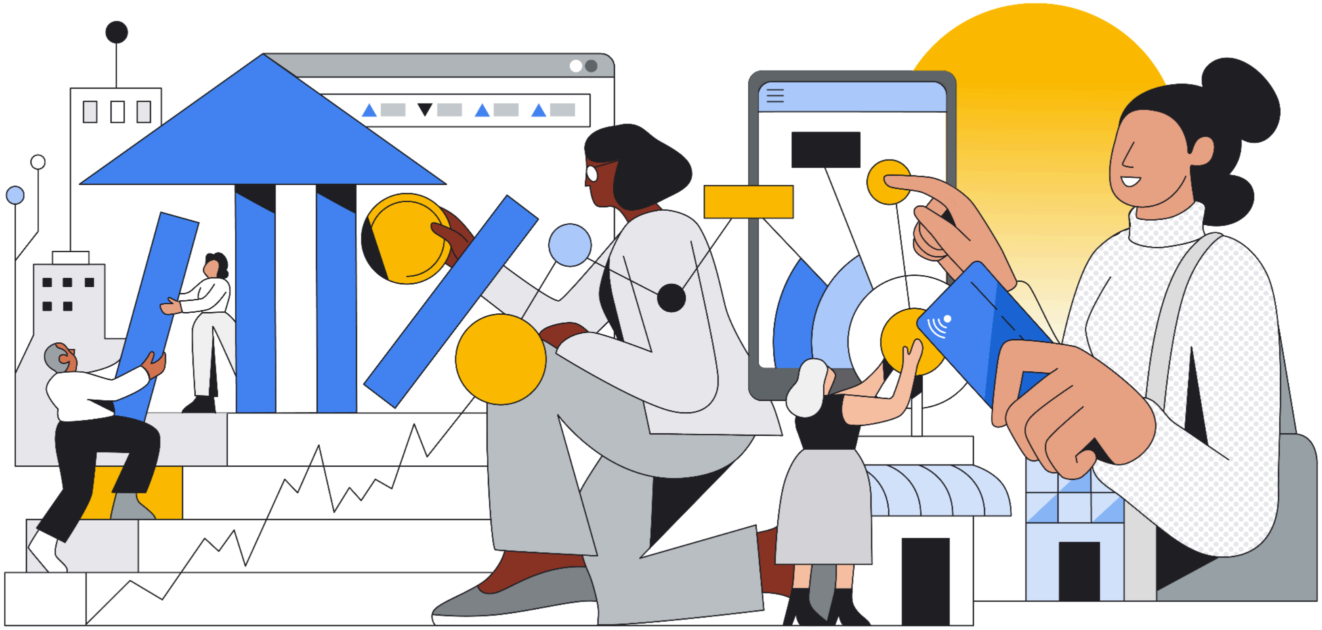

Table of Contents

Disclaimer

This content was last updated in March 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 banks and financial institutions 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 Commercial Banks in India, regulated by the Reserve Bank of India (RBI), in securely adopting and expanding their use of Google Cloud amidst the evolving digital landscape of the financial sector. 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 RBI Master Directions which is released in Nov, 2025 for Commercial Banks:

- Reserve Bank of India (Commercial Banks – Managing Risks in Outsourcing) Directions, 2025

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 the Reserve Bank of India'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 RBI guidelines generally place significant emphasis on key aspects of IT governance and IT service provider management, 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 banks, 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 (RBI) 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 bank's that help them comply with the contractual requirements under the RBI 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 RBI Outsourcing Guidelines

The below mapping is designed to help Commercial Banks regulated by the Reserve Bank of India ("regulated entity" or "regulated entities") with the information on how Google Cloud supports them with the requirements under the Reserve Bank of India (Commercial Banks – Managing Risks in Outsourcing) Directions, 2025 ("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: **Chapter IV – Outsourcing of Information Technology (IT) Services** - D. Risk Management, E. Outsourcing Process, F. Specific Outsourcing Arrangements.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	**D. Risk Management**		
2	**D.1 Risk Management Framework**		
3	60. A bank shall put in place a risk management framework that comprehensively deals with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with such IT outsourcing arrangements.	Our shared responsibility and shared fate page on Google Cloud 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. Additional details on meeting regulatory, compliance and privacy needs can be seen here.	N/A
4	61. A bank shall suitably document risk assessments with necessary approvals in line with the roles and responsibilities of the Board of Directors, Senior	Our Risk Governance of Digital Transformation provides practical guidance to Board of Directors, and Senior Management through the transformational activities that will be taking place within your	N/A

	Management, and IT Function, and subject the same to internal and external quality assurance on a periodic basis as determined by the Board-approved policy	organization, and what in turn those mean for your functions and their own transformations and how to best position your risk, compliance and audit programs for success in the cloud. You can also refer to the Board of Directors Handbook for Cloud Risk Governance for more details.	
5	62. A bank shall effectively assess the impact of concentration risk posed by multiple outsourcing arrangements to the same service provider and the concentration risk posed by outsourcing critical or material functions to a limited number of service providers.	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)
6	**D.2 Confidentiality and Security of Information**		
7	63. A bank shall be responsible for the confidentiality, and integrity of data and information pertaining to its customers that are available to the service provider.	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.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

		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 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	Certifications and Audit Reports

		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 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	Significant Developments Data Incidents (Cloud Data Processing Addendum) Ongoing Performance Monitoring

		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.	Business Continuity and Disaster Recovery
8	64. In this regard, a bank shall adhere to directions stated in paragraph 23 to paragraph 26 of these Directions and additionally ensure that:		
9	1) access by service providers to data at the bank, or its data centre shall be on 'need to know' basis, with appropriate controls to prevent security breaches or data misuse;	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.	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.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
10	2) in the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the bank remains responsible for understanding and monitoring the control environment of all service providers that have access to its data, systems, records, or resources;	Bank's can keep a surveillance over any activity taking place in their Google Cloud account through the admin center.	N/A
11	3) it immediately notifies RBI in the event of breach of security, and leakage of confidential customer-related information. In these eventualities, the bank shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.	Control processes and security practices For more information on security practices and control processes, refer to Row 7 and 8. Security breaches 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 Data Incidents (Data Processing and Security Terms)

		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.	
12	65. With regard to requirement that the data should not be combined or comingled, as stipulated in paragraph 26, it would suffice if there is clear separation and isolation of data (bank, and its customer specific data and information) to ensure that only the personnel as authorised by the bank is able to access data that belongs to them in a multi-tenant environment / architecture.	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)
13	**E. Outsourcing Process**		
14	**E.1 Service Provider Evaluation**		
15	66. The directions regarding service provider evaluation as applicable to outsourcing of financial services contained in paragraph 29 to paragraph 31 shall apply, mutatis mutandis, to outsourcing of IT services, with the following additional considerations:		
16	i) technology, infrastructural stability, data backup arrangements, and disaster recovery plan;	Refer row 7	
17	ii) conflict of interest, if any;	This is a customer consideration	
18	iii) capability to identify, and segregate bank's data;	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	iv) capability to comply with the regulatory and legal requirements of the outsourcing arrangement;	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.	Enabling Customer Compliance

		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.	
20	v) information / cyber security risk assessment;	Refer to row 7.	N/A
21	vi) ensuring that appropriate controls, assurance requirements, and possible contractual arrangements are in place to ensure data protection and bank's access to the data which is processed, managed or stored by the service provider;	Data protection, controls and assurance Refer to Row 7. Access to Data 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.	Enabling Customer Compliance
22	vii) ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and	Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Services Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
23	viii) ability to enforce agreements, and the rights available thereunder including those relating to aspects such as data storage, data protection, and confidentiality.	Refer to your Google Cloud Financial Services Contract.	Governing Law
24	67. A bank should adopt a risk-based approach in conducting such due diligence activities.	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	N/A

		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.	
25	**E.2 Outsourcing Agreement**		
26	68. A bank shall ensure that its rights and obligations and those of each service provider are clearly defined and set out in a legally binding written agreement, in line with the provisions specified in paragraph 33 of these Directions. In principle, the provisions of the agreement shall appropriately reckon the criticality of the outsourced task to the business of the bank, the associated risks, and the strategies for mitigating or managing them.	The rights and obligations of 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.	Definitions
27	69. In addition to the requirements specified in subparagraphs (i) to (vii) of paragraph 34, a bank shall also include at minimum (as applicable to the scope of Directions in this Chapter) the following aspects in any agreement for outsourcing of IT services:		
28	i) provisions covering service provider's subcontractors with respect to service and performance standards [subparagraph (i) of paragraph 34] and bank's right to conduct audits [subparagraph (vii) of paragraph 34];	Google's subcontractors are responsible to ensure compliance with applicable laws. Google is committed to working with the banks in assisting to fulfil the audit requirements vis-a-vis the subcontractors.	Google Subcontractors - Compliance
29	ii) access by the bank to all data, books, records, information logs, alerts, and business premises relevant to the outsourced service, available with the service provider;	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.	Regulator Information, Audit and Access

30	iii)	type of material adverse events (e.g., data breaches, denial of service, and service unavailability, relevant to the outsourced services) and the incidents required to be reported to the bank, to enable the bank to take prompt risk mitigation 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 (Cloud Data Processing Addendum)
31	iv)	compliance with the provisions of Information Technology Act, 2000, and other applicable legal requirements and standards to protect the customer data;	Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services	Representations and Warranties
32	v)	the deliverables including Service Level Agreements (SLAs) formalising 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
33	vi)	storage of data only in India (as applicable) as per extant regulatory requirements;	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. For more details, go through our Data boundary via Assured Workloads page.	Data Location (Service Specific Terms)
34	vii)	clauses requiring the service provider to provide details of data (related to the bank and its customers) captured, processed, and stored;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data. 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.	Data Security; Google's Security Measures; (Cloud Data Processing Addendum)

35	viii)	types of data / information that the service provider (vendor) is permitted to share with bank's customer 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
36	ix)	the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;	Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority. 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. 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.	Term and Termination Support through Resolution Services; Liability; Indemnification
37	x)	contingency plan(s) to ensure testing requirements;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery.
38	xi)	right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;	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 Subcontractors

		Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	
39	xii) right of RBI or person(s) authorised by it to perform inspection of the service provider and any of its sub-contractors and access the bank's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider / or its sub- 32 contractors, in relation and as applicable to the scope of the outsourcing arrangement;	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. Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	Regulator Information, Audit and Access Google Subcontractors
40	xiii) clauses making the service provider contractually liable for the performance and risk management practices of its subcontractors;	Google will remain liable to you for any subcontracted obligations.	Google Subcontractors.
41	xiv) obligation of the service provider to comply with directions issued by the RBI in relation to the services outsourced to the service provider, through specific contractual terms and conditions specified by the bank;	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. Google will comply with the regulated entity's instructions.	Instructions Scope of Processing; Customer's Instructions (Cloud Data Processing Addendum)
42	xv) termination rights of the bank, including the ability to orderly transfer the proposed outsourcing arrangement to another service provider, 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	Term and Termination Transition Term

		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.	Transition Assistance
43	xvi) obligation of the service provider to co-operate with the relevant authorities in case of insolvency or resolution of the bank;	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 as per terms of the agreement.	Support through Resolution
44	xvii) provision to consider skilled resources of service provider who provide core services as 'essential personnel' so that a limited number of staff with backup arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);	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 -emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) -pandemics	Business Continuity and Disaster Recovery
45	xviii) clause requiring suitable back-to-back arrangements between service providers and the OEMs; and	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.	Google Subcontractors
46	xix) clause requiring non-disclosure agreement with respect to information retained by the service provider	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Confidentiality
47	**E.3 Monitoring and Control of Outsourced Services**		
48	70. A bank shall have in place a management structure to monitor and control its outsourced services.	Monitoring	

		This shall include (as applicable to the scope of Directions in this Chapter), but not be limited to, monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, and incident response mechanism	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). 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.	Ongoing Performance Monitoring Significant Developments Data Incidents (Data Processing and Security Terms)
49	71.	A bank shall conduct regular audits (as applicable to the scope of Directions in this Chapter), of service providers (including subcontractors) with regard to the service 33 outsourced by it. Such audits may be conducted either by bank's internal	Google grants audit, access and information rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.	Customer Information, Audit and Access

	or external auditors appointed to act on bank's behalf.	In addition, Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
50	72. While outsourcing various IT services, more than one RE may be availing services from the same third-party service provider. In such scenarios, in lieu of conducting separate audits by individual REs of the common service provider, they may adopt pooled (shared) audit. This allows the relevant REs to either pool their audit resources or engage an independent third-party auditor to jointly audit a common service provider. However, in doing so, it shall be the responsibility of REs in ensuring that the audit requirements related to their respective contract with the service provider are met effectively.	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities.	N/A
51	73. The audits shall assess, inter alia, the performance of the service provider, adequacy of the risk management practices adopted by the service provider, and compliance with laws and regulations. The frequency of the audit shall be determined based on the nature and extent of risk, and impact on the bank from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management, and in case of any adverse development, the same shall be put up to the Board for information.	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. 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.	Customer Information, Audit and Access
52	74. A bank, depending upon the risk assessment, may also rely upon globally recognised third-party certifications made available by the service provider in lieu of conducting independent audits. However, this shall not absolve the bank of its responsibility in ensuring assurance on the controls and procedures required to safeguard	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)	Certifications and Audit Reports

	data security (including availability of systems) at the service provider's end.	-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	
53	75. A bank shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its obligations. A bank shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, security, and operational resilience preparedness.	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 on our Incidents & the Google Cloud dashboard page. You can review Google's audited financial statements on Alphabet's Investor Relations page.	Significant Developments
54	76. A bank shall ensure that the service provider grants unrestricted and effective access to (a) data related to the outsourced services; (b) the relevant business 34 premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight by the bank, its auditors, RBI, and other relevant Competent Authorities, as authorised under law.	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.	Regulator Information, Audit and Access Customer Information, Audit and Access Enabling Customer Compliance
55	**E.4 Inventory of Outsourced Services**		
56	77. A bank shall create an inventory of IT services outsourced to service providers (including key entities involved in their supply chains). Further, the bank shall map its dependency on third parties and periodically evaluate the information received from the service providers.	Google will map its dependencies and periodically evaluate the information from all sub contractors, oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors

57	**E.5 Business Continuity and Management of Disaster Recovery Plan**		
58	78. The Directions regarding 'Business Continuity and Management of Disaster Recovery Plan' as applicable to outsourcing of financial services contained in paragraph 4140 to paragraph 43 shall apply, mutatis mutandis, to outsourcing of IT services. The Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for outsourced IT services shall be commensurate with the nature and scope of the outsourced service as per extant instructions issued by RBI from time to time on BCP / DR requirements.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
59	**E.6 Exit Strategy**		
60	79. The IT outsourcing policy shall contain a clear exit strategy for ensuring business continuity during and after exit.	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. -Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by on-premise.	Data Export (Cloud Data Processing Addendum)

		-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.	
61	80. The strategy shall include plans for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary.	Refer to row 60	N/A
62	81. In documenting its exit strategy, a bank shall, inter alia, identify alternative arrangements, which may include performing the service by a different service provider, or by the bank itself.	Refer to row 60	N/A
63	82. A bank shall ensure that outsourcing agreements have necessary clauses on safe removal or destruction of data, hardware and all records (digital and physical), as applicable. Further, the outsourcing agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering, or changing any 35 data during the transition period, unless specifically advised by the regulator or the concerned bank.	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. Transition 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 this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.	Deletion on Termination (Cloud Data Processing Addendum) Transition Term Transition Assistance

		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 will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	
64	83. A service provider shall be legally obliged to cooperate fully with both the bank and its new service provider(s) to ensure there is a smooth transition.	Transition 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 this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. 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 will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Term Transition Assistance
65	**E.7 Termination**		
66	84. In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the bank, the same shall be given due publicity by the bank so as to ensure that the customers stop dealing with the concerned service provider.	Upon termination of the outsourcing agreement, the GCP Admin should ensure that the end users are informed. 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)
67	**F. Specific Outsourcing Arrangements**		
68	**F.1 Outsourcing within a Group / Conglomerate**		
69	85. A bank may outsource any IT service within its business group / conglomerate, provided that such	These are responsibilities of the bank.	NA

	an arrangement is backed by the Board-approved policy and appropriate SLAs / agreements with its group entities are in place.		
70	86. The selection of a group entity shall be based on objective reasons that are similar to selection of a third-party, and the bank shall appropriately deal with any conflicts of interest that such an outsourcing arrangement may entail.		NA
71	87. A bank, at all times, shall maintain an arm's length relationship in dealings with its group entities. Risk management practices being adopted by the bank while outsourcing to a group entity shall be identical to those specified for a non-related party.		NA
72	**F.2 Offshore or Cross-Border outsourcing**		
72	88. In principle, outsourcing arrangements shall only be entered into with parties operating in jurisdictions that uphold confidentiality clauses and agreements.	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. Google will ensure its subcontractors comply with Google's security measures and that all persons authorized to process customer data are under an obligation of confidentiality. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors Data Security; Access and Compliance (Cloud Data Processing Addendum)
74	89. While engaging with service provider(s) in a foreign country, a bank shall:		
75	i) closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, and establish sound procedures for mitigating the country risk.	Service location To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities.	N/A

	This includes, inter alia, having appropriate contingency and exit strategies;	● Information about the location of Google's facilities and where individual GCP services can be deployed is available here. ● Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: ● The same robust security measures apply to all Google facilities, regardless of country / region. ● Google makes the same commitments about all its subprocessors, regardless of country / region. To help comply with data residency requirements, Google Cloud gives you the ability to control the regions where data at rest is stored.Once you choose where to store your data, Google will not store it outside your chosen region(s). For more details, go through our Data boundary via Assured Workloads page. Contingency and exit planning Refer to row 60 for more information on Google's exit planning.	
76	ii) clearly specify the governing law of the outsourcing arrangement;	Refer to your Google Cloud Financial Services Contract.	Governing Law
77	iii) ensure that availability of records to the bank and the RBI will not be affected even in case of liquidation of the service provider;	You retain all intellectual property rights in your data. 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:	Term and Termination

		• Google Kubernetes Engine (GKE) 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. In the unlikely event of Google's insolvency, RE's can refer to the contractual commitments made by Google when dealing with the appointed insolvency practitioner.	
78	iv) ensure the right of the bank and RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction; and	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.	Regulator Information, Audit and Access Customer Information, Audit and Access
79	v) ensure that the arrangement complies with all statutory requirements as well as regulations issued by the RBI 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. 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
80	**F.3 Outsourcing of Security Operations Centre (SOC)**		
81	90. Considering the risks associated with outsourcing of Security Operations Centre (SOC) operations		

	by a bank, such as data being stored and processed at an external location and managed by the service provider (or its subcontractors) to which the bank has lesser visibility, the bank, to mitigate the risks, shall adopt the following requirements in the case of outsourcing of SOC operations in addition to the controls prescribed in this Chapter:		
82	i) unambiguously identify the owner of assets used in providing the services (e.g., systems, software, source code, processes, and concepts);	Google Cloud undergoes annual independent third party audits on a regular basis and these checks are performed as part of the audits.	Certifications and Audit Reports
83	ii) ensure that the bank has adequate oversight and ownership over the rule definition, customisation and related data / logs, meta-data and analytics (specific to the bank);	Google Cloud services write audit logs that record administrative activities and accesses within your Google Cloud resources. Banks having resources and workloads on Google Cloud will have full access and ownership of all the audit logs in their admin centers. - https://docs.cloud.google.com/logging/docs/audit	N/A
84	iii) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored or processed periodically;	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. 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	Customer Information, Audit and Access. Certifications and Audit Reports

		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.	
85	iv) integrate the outsourced SOC reporting and escalation process with the bank’s incident response process; and	Google will notify you of data incidents promptly and without undue delay. More information on Google’s data incident response process is available here. To assist customers with their own incident response, Google's notification will describe: ● the nature of the Data Incident including the Customer resources impacted; ● the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; ● the measures, if any, Google recommends that Customer take to address the Data Incident; and ● details of a contact point where more information can be obtained. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. OurAgentic SOC: ● delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. ● enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution.	Data Incidents (Cloud Data Processing Addendum)

		Information on Google's security products is available here. 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. ● Cloud Security Health Analytics provides visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	
86	v) review the process of handling of the alerts or events.	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. Bank's can access the audit reports from the Compliance reports manager where the details can be reviewed.	N/A
87	**F.4 Usage of Cloud Computing Services**		
88	91. Several cloud deployment and service models have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. (1) Example - 1: (i) Some cloud services are: (a) Infrastructure as a Service (IaaS): The service provides computing, storage, network, and other basic resources so that the client can develop and deploy their applications. (b) Platform as a Service (PaaS): The service provides software for building application, middleware, database, development environment, and other tools along with the infrastructure to the client. (c) Software as a Service (SaaS): Client uses the application(s) provided by the service provider on a cloud infrastructure. (ii) Besides the three common application services, Cloud Service Providers (CSPs) also provide a	Google Cloud is a public cloud service. It provides Infrastructure as a Service, Platform as a Service, Software as a Service, Database as a Service, Security as a Service, Storage as a Service and others, with varying feature and service levels. Customers can choose to deploy Google Cloud as part of a hybrid or multi-cloud deployment.	

		range of services, viz., Database as a Service, Security as a Service, Storage as a Service, and others with varying risk levels. (2) Example - 2: Some of the popular deployment models for delivery of cloud services are Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud.		
89	92.	Considering the varied services, benefits, and risk profiles associated with the cloud deployment and service models, a bank that uses cloud services for storage, computing and movement of data in cloud environments shall, in addition to other applicable provisions in these Directions:		
90	i)	undertake a comprehensive assessment of its business strategy and goals adopted to the existing IT applications' footprint and associated costs. Such assessment shall include, but not be limited to, an analysis of various heads of cloud-related expenditure, such as application refactoring, integration, consulting, migration, and projected recurring expenditure depending on the nature of workloads. The extent of cloud adoption may vary, ranging from migration of non-business critical workloads to the cloud, to deployment of critical business applications such as SaaS, or other combinations in between, and shall be determined based on a duly conducted business technology risk assessment;	Google recognizes that you need to plan and execute your migration carefully. Our Migrate 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 Risk Assessment & Critical Asset Discovery solution from Google Cloud's Security and Resilience offerings evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A
91	ii)	ensure, inter alia, that the 'IT outsourcing policy', referred to in paragraph 57 of these Directions, addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, to its entry into the cloud, and till the data is permanently erased or deleted. It shall also ensure that specified procedures are consistent with business needs, and legal and regulatory requirements;	The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment.	N/A

			In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Risk Governance of Digital Transformation whitepaper and Adapting model risk management for financial institutions in the generative AI era whitepaper for more information, including about how control design and ownership evolves in the cloud.	
92	iii)	take into account cloud service specific factors, viz., multi-tenancy, and multilocation storing or processing of data, and attendant risks while establishing appropriate risk management framework;	This is addressed in the Cloud Data Processing Addendum.	Cloud Data Processing Addendum
93	iv)	implement necessary controls by referring to the cloud security best practices, as per applicability of the shared responsibility model between the bank and the Cloud Service Provider (CSP); For cloud security best practices, a bank may refer to, inter alia, NIST SP 800- 210 General Access Control Guidance for Cloud Systems https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. 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. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	N/A

		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	
94	v) put in place strong cloud governance by adopting and demonstrating a wellestablished and documented cloud adoption policy. Such a policy shall, inter alia, (a) identify the services that can be moved to the cloud; (b) enable and support protection of various stakeholder interests; (c) ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability, and data storage requirements, aligned with data classification; and (d) provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs;	Refer to Rows 7, 99 to 105. Our Risk Governance of Digital Transformation whitepaper provides a guide for Chief Risk Officers, Chief Compliance Officers and Heads of Internal Audit of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
95	vi) ensure that the selection of a CSP is based on a comprehensive risk assessment of the CSP. A bank shall enter into a contract only with CSPs that are subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to the bank, including those relating to aspects such as data storage, data protection, and confidentiality;	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.	N/A
96	vii) ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised	Cloud infrastructure resilience Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening Operational Resilience in	N/A

	architecture principles and standards. The technology architecture shall: (a) provide for a standard set of tools and processes to manage containers, images, and releases; (b) provide for a secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the bank; (c) be protected against data integrity and confidentiality risks, and against co-mingling of data, in case of multi-tenancy environments; and (d) be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data / information security;	Financial Services by Migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our FSI Perspective - Reliability page explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. Cloud application resilience Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications Encryption You can choose to use these encryption and key management tools 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. ● 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. Data segregation To keep data private and secure, Google logically isolates each customer's data from that of other customers.	
97	viii) agree upon the Identity and Access Management (IAM) with the CSP and ensure that role-based access to the cloud hosted applications, both in respect of user-access and privileged-access, is provided. The bank shall: (a) establish stringent access controls, as applicable for an on-premises application, for IAM for cloud-based applications; (b) implement segregation of duties, role conflict matrix for all kinds of user-access, and privileged-access roles in the cloud-hosted application irrespective of the cloud service model; (c) ensure that access provisioning is governed by principles of 'need to know', and 'least privileges'; and (d) implement multi-factor authentication for access to cloud applications;	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. ● 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.	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.	
98	ix) ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in or by an on-premises application. This includes ensuring secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the bank, and necessary procedures to authorise changes to cloud applications and related resources;	Security controls Refer to Row 7 for information about Google's security practices and tools. Network security 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 Security? page. 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. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic	Data Security; Google's Security Measures (Cloud Data Processing Addendum) Access and Site Controls (Cloud Data Processing Addendum)

		signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information. Configuration management and monitoring There are a number of ways to perform effective configuration management using the services: ● Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources. ● Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. ● Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. ● Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints. ● Security Command Center allows you to proactively manage risks and respond to threats with posture management and threat detection for AI, infrastructure, and data. Our Risk and Compliance as Code (RCaC) Solution stack enables compliance and security control automation through a combination of Google Cloud Products, Blueprints, Partner Integrations, workshops and services to simplify and accelerate time to value.	

		Through the RCaC solution, customers can introduce automation via IaC (Infrastructure as Code) and PaC (Policy as Code) in the form of blueprints. This lays the foundation of preventative controls. The next level of maturity is detection as code which involves monitoring for (security and compliance) drifts and applying remediations when an out-of-compliance infrastructure is identified. This forms a continuous monitoring loop that helps prevent misconfigurations. AI Security Google's Secure AI Framework (SAIF) is a framework for securing AI systems throughout their lifecycles. SAIF is designed for practitioners – the security professionals, developers, and data scientists on the front lines – to ensure AI models and applications are secure by design. More details in the technical paper about implementing Secure AI Framework Controls in Google Cloud.	
99	x) define minimum monitoring requirements in the cloud environment and assess the information / cyber security capability of the CSP, to ensure that it:	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.	N/A
100	a) maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;	Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security	N/A

		threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments. Refer to our security whitepaper for more information.	
101	b) is able to maintain its information / cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets, or its business environment;	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. 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.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
102	c) has set the nature and frequency of testing of controls in respect of the outsourced services commensurate with the materiality of the services being outsourced by the bank and the threat environment; and	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)	Customer Penetration Testing Certifications and Audit Reports

		- 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.	
103	d) has mechanisms in place to assess the subcontractors with regards to confidentiality, integrity, and availability of the data being shared with them, where applicable;	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. Google will ensure its subcontractors comply with Google's security measures and that all persons authorized to process customer data are under an obligation of confidentiality. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors Data Security; Access and Compliance (Cloud Data Processing Addendum)
104	xi) ensure appropriate integration of logs and events from the CSP into the bank's SOC, wherever applicable and retention of relevant logs in cloud for incident reporting and handling of incidents relating to services deployed on the cloud;	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available here. To assist customers with their own incident response, Google's notification will describe: - the nature of the Data Incident including the Customer resources impacted; - the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; - the measures, if any, Google recommends that Customer take to address the Data Incident; and - details of a contact point where more information can be obtained.	Data Incidents (Cloud Data Processing Addendum)

		In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. This also addresses A-14 (under Chapter III of the Outsourcing of Information Technology (IT) Services) about cyber incident reporting. OurAgentic SOC: ● delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. ● enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. 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. ● Cloud Security Health Analytics provides visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	
105	xii) ensure that the cyber resilience controls of the CSP complement the bank's own application security measures, and that both the bank and the CSP maintain continuous and regular updates of security-related software, including upgrades, fixes, patches, and service packs, to safeguard applications against advanced threats and malware;	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.	N/A

		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. 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.	
106	xiii)	ensure that the CSP has a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities;	Refer to Rows 99 to 105.	
107	xiv)	ensure that the business continuity framework provides for continued operation of critical functions in the event of a disaster affecting the bank's cloud services or failure of the CSP, with minimal disruption to services, and without compromising data integrity and security;	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 Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. ● Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. ● Google Distributed Cloud: is a portfolio of hardware and software solutions that provides customers an option to extend Google Cloud infrastructure to the edge and into their data centers. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer Google Cloud Data Portability and Switching Procedures to understand more on transparent and flexible methods for managing and moving data, and also Data Transfer Essentials which offers a cost-effective way to move data between the services of an application	Data Export (Cloud Data Processing Addendum)

			that resides across multiple CSPs, while adhering to regulatory requirements.	
108	xv)	ensure that the CSP has put in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them through, inter alia, robust incident response and recovery practices including conduct of DR drills at various levels of cloud services including necessary stakeholders;	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. Google recognizes the importance of regular testing in the context of operational resilience. Google runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests our operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability. Refer to the Google Cloud Security & Resilience Framework to understand more on the Comprehensive solutions for every phase of the security and resilience lifecycle, help protect critical assets in cloud and on-premise, modernize your security protections, and enable rapid recovery wherever your assets reside.	Business Continuity and Disaster Recovery
109	xvi)	develop an exit strategy that shall		
110	a)	factor, inter alia, agreed processes and turnaround times for returning the bank's service collaterals and data held by the CSP; data completeness and portability; secure purge of bank's information from the CSP's environment; smooth transition of services; and unambiguous definition of liabilities, damages, penalties and indemnities, 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 Transfer Essentials which offers a cost-effective way to move data between the services of an application	Data Export (Cloud Data Processing Addendum)

	also be a part of the service level stipulations in SLA;	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, 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	Deletion on Termination (Cloud Data Processing Addendum) Transition Term

		provide the Services for 12 months beyond the expiry or termination of the contract. Service credits If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Liabilities Refer to your Google Cloud Financial Services Contract. Indemnities Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Services Liability Indemnification
111	b) include exit plans which align with the ongoing design of applications and service delivery technology stack;	Configuration management and monitoring There are a number of ways to perform effective configuration management using the services: ● Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources. ● Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. ● Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. ● Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.	N/A

		Our Risk and Compliance as Code (RCaC) Solution stack enables compliance and security control automation through a combination of Google Cloud Products, Blueprints, Partner Integrations, workshops and services to simplify and accelerate time to value. Through the RCaC solution, customers can introduce automation via IaC (Infrastructure as Code) and PaC (Policy as Code) in the form of blueprints. This lays the foundation of preventative controls. The next level of maturity is detection as code which involves monitoring for (security and compliance) drifts and applying remediations when an out-of-compliance infrastructure is identified. This forms a continuous monitoring loop that helps prevent misconfigurations. 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 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.	
112	c) include contractually agreed exit / termination plans, which specify how the cloud-hosted service(s) and data will be moved out from the	Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their	Transition Term

		cloud with minimal impact on continuity of the bank's business, while maintaining integrity and security; and	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. 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 will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance
113	d)	include clauses for prompt take-over of all records of transactions, customer and operational information, and configuration data, in a systematic manner from the CSP, and purging at the CSP end, and ensuring independent assurance before signing off from the CSP.;	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)
114	xvii)	ensure that the audit / periodic review / third-party certifications cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities of both bank and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response, and resilience preparedness and testing.	Audit 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.	Customer Information, Audit and Access.
			Third party certifications 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:	Certifications and Audit Reports

		• 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.	

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 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 RBI 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.