Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

This document is designed to help Regulated Entities supervised by the Reserve Bank of India ("**regulated entity**") to consider the Reserve Bank of India Master Direction on Outsourcing of Information Technology Services 2023 ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Chapter IV - (Evaluation and Engagement of Service Providers), Chapter V - (Outsourcing Agreement), Chapter VI - (Risk Management), Chapter VII - (Monitoring and Control of Outsourced Activities), Chapter – IX (Cross-Border Outsourcing), Chapter - X (Exit Strategy) and Appendix – I (Usage of Cloud Computing Services). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	**Chapter IV - Evaluation and Engagement of Service Providers**		
2	13. **Due Diligence on Service Providers**		
3	a) In considering or renewing an Outsourcing of IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below.	N/A
4	b) A risk-based approach shall be adopted 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 Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A
5	c) Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. Where possible, the RE shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.	Financial and operational information You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. You can review Google's audited financial statements on Alphabet's Investor Relations page. Information about Google Cloud's leadership team is available on our Media Resources page. Independent reviews and market feedback Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance.	
6	d) REs shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.	Google recognizes the importance of continuity for regulated firms 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 Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
7	14. **Aspects to be considered**		
8	Due diligence shall involve evaluation of all available information, as applicable, about the service provider, including but not limited to:		
9	a) past experience and demonstrated competence to implement and support the proposed IT activity over the contract period;	Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about Google Cloud's leadership team is available on our Media Resources page.	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
10	b) financial soundness and ability to service commitments even under adverse conditions;	You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A
11	c) business reputation and culture, compliance, complaints and outstanding or potential litigations;	Reputation Refer to Row 9 for more information on Google's business reputation. Culture You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organizational policies e.g. our Code of Conduct Compliance Compliance Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services. You can review information about how Google addresses key compliance requirements at our Google Cloud Compliance Resource Center. Potential litigation and complaints Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A N/A Representations and Warranties N/A
12	d) conflict of interest, if any;	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct, which addresses conflicts of interest.	N/A
13	e) external factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.	Data Transfers (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s) You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Security; Subprocessors (Cloud Data Processing Addendum) Data Transfers (Cloud Data Processing Addendum)
14	f) details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;	Infrastructure and security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security and confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. • Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page.	

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints Internal control and audit coverage Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Reporting Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Certifications and Audit Reports Significant Developments

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 in our Data incident response whitepaper. 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 Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services. ● Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Data back-up Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. Business Continuity Management Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Data Incidents (Cloud Data Processing Addendum) Ongoing Performance Monitoring Business Continuity and Disaster Recovery
15	g) capability to identify and segregate REs data;	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
16	h) quality of due diligence exercised by the service provider with respect to its employees and sub-contractors;	Employees Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. Subcontractors Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. • Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	N/A Google Subcontractors
17	i) capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services 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. 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
18	j) information/ cyber security risk assessment;	Refer to Row 14.	N/A
19	k) ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider;	Data protection, controls and assurance Refer to Row 14. 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
20	l) 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.	Services

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
21	m) 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
22	**Chapter – V Outsourcing Agreement**		
23	15. **Legally binding agreement**		
24	a) REs shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
25	b) In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the RE, the associated risks and the strategies for mitigating or managing them.	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
26	c) The terms and conditions governing the contract shall be carefully defined and vetted by the RE's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the RE to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance
27	d) The agreement shall also bring out the nature of legal relationship between the parties.	See above.	N/A
28	16. **Aspects to be considered in agreement**		
29	The agreement at a minimum should include (as applicable to the scope of Outsourcing of IT Services) the following aspects:		

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
30	a) details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any;	Services The GCP services are described here. Service Levels The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. Subcontractors Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Definitions Services Google Subcontractors
31	b) effective access by the RE to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, 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
32	c) regular monitoring and assessment of the service provider by the RE for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
33	d) type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to RE to enable RE 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 in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
34	e) compliance with the provisions of Information Technology Act, 2000, 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
35	f) 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
36	g) storage of data (as applicable to the concerned REs) only in India as per extant regulatory requirements;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
37	h) clauses requiring the service provider to provide details of data (related to RE 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)
38	i) controls for maintaining confidentiality of data of RE's and its customers', and incorporating service provider's liability to RE in the event of security breach and leakage of such information;	Confidentiality This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 14 for more information about the security of our services. Liability Refer to your Google Cloud Financial Services Contract.	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum) Liability
39	j) types of data/ information that the service provider (vendor) is permitted to share with RE'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. Google engages third party vendors to perform limited activities in connection with the services. Information about these vendors (including their locations) and the limited processing of customer data they are authorized to perform is available on our Google Cloud Platform Subprocessor page.	N/A
40	k) specifying 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.	Term and Termination Support through Resolution Services; Liability; Indemnification

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
41	l) contingency plan(s) to ensure business continuity and 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.
42	m) right to conduct audit of the service provider (including its sub-contractors) by the RE, whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the RE;	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. 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 recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Customer Information, Audit and Access Google Subcontractors Certifications and Audit Reports

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
43	n) 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 will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors
44	o) recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow RBI or person(s) authorised by it to access the RE's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and/ or its sub-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
45	p) including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors;	Google will remain liable to you for any subcontracted obligations.	Google Subcontractors.
46	q) obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the RE;	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)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
47	r) clauses requiring prior approval/ consent of the RE for use of sub-contractors by the service provider for all or part of an outsourced activity;	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services they use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.	Google Subcontractors
48	s) termination rights of the RE, including the ability to orderly transfer the proposed IT-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 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.	Term and Termination Transition Term Transition Assistance
49	t) obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the RE;	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.	Support through Resolution
50	u) provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff with back-up 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	Business Continuity and Disaster Recovery

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		-emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) -pandemics	
51	v) 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
52	w) 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
53	**Chapter – VI Risk Management**		
54	17. **Risk Management Framework**		
55	(a) REs shall put in place a Risk Management framework for Outsourcing of IT Services that shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements.	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
56	(b) The risk assessments carried out by the REs shall be suitably documented with necessary approvals in line with the roles and responsibilities for the Board of Directors, Senior Management and IT Function. Such risk assessments shall be subject to internal and external quality assurance on a periodic basis as determined by the Board-approved policy.	Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
57	(c) REs shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the service provider.	Refer to Row 14 for more information on Google's security practices.	N/A
58	(d) Access to data at RE's location / data centre by service providers shall be on need-to-know basis, with appropriate controls to prevent security breaches and/or data misuse.	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 against unauthorized access by controlling access rights and roles for Google Cloud Platform resources.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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 "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies. 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)
59	(e) Public confidence and customer trust in REs is a prerequisite for their stability and reputation. Hence, REs shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. Access to customer information by staff of the service provider shall be on need-to-know basis.	Refer to Rows 14 and 58..	N/A
60	(f) In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the RE remains responsible for understanding and monitoring the control environment of all service providers that have access to the RE's data, systems, records or resources.	This is a customer consideration.	N/A
61	(g) In instances where a service provider acts as an outsourcing agent for multiple REs, care shall be taken to build adequate safeguards so that there is no combining of information, documents, records and assets.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
62	(h) The RE shall ensure that cyber incidents are reported to the RE by the service provider without undue delay, so that the incident is reported by the RE to the RBI within 6 hours of detection by the TPSP.	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 in our Data incident response whitepaper.	Significant Developments Data Incidents (Data Processing and Security Terms)
63	(i) The REs shall review and monitor the control processes and security practices of the service provider to disclose security breaches. The REs shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, REs 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 14. Security breaches Refer to Row 62.	N/A
64	(j) Concentration Risk: REs shall effectively assess the impact of concentration risk posed by multiple outsourcings to the same service provider and/or 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 Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	Data Export (Cloud Data Processing Addendum)
65	18. **Business Continuity Plan and Disaster Recovery Plan**		
66	a) REs shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity 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

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
67	b) In establishing a viable contingency plan, REs shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.	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. ● Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)
68	c) In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/liquidation of the service provider, REs shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.	Refer to Row 67.	N/A
69	d) REs shall ensure that service providers are able to isolate the REs' information, documents and records and other assets. This is to ensure that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the RE can be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.	To keep data private and secure, Google logically isolates each customer's data from that of other customers. 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.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum) Deletion on Termination (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
70	**Chapter – VII Monitoring and Control of Outsourced Activities**		
71	19. **Monitoring and Control of Outsourced Activities**		
72	a) REs shall have in place a management structure to monitor and control its Outsourced IT activities. This shall include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.	Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). 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 in our Data incident response whitepaper.	Ongoing Performance Monitoring Significant Developments Data Incidents (Data Processing and Security Terms)
73	b) RE shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by RE's internal auditors or external auditors appointed to act on RE's behalf.	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 Google Subcontractors

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
74	c) 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. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.	N/A
75	d) The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact to the RE 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
76	e) REs, 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 REs of their responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001:2013 (Information Security Management Systems) -ISO/IEC 27017:2015 (Cloud Security) -ISO/IEC 27018:2014 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources	Certifications and Audit Reports

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
77	f) The RE shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. RE shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in 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
78	g) In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the RE, the same shall be given due publicity by the RE so as to ensure that the customers stop dealing with the concerned service provider.	Given the nature of the services, Google does not have direct interaction with the regulated entity's customers.	N/A
79	h) REs shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the REs, their auditors, regulators 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
80	**Chapter – IX Cross-Border Outsourcing**		
81	21. **Additional requirements for Cross-Border Outsourcing**		
82	a) The engagement of a service provider based in a different jurisdiction exposes the RE to country risk. To manage such risk, the RE shall 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, as well as establish sound procedures for mitigating the country risk. This includes, *inter alia*, having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the RE and the RBI will not be affected even in case of liquidation of the service provider.	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. • 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.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. Contingency and exit planning Refer to Rows 87 to 89 for more information on Google's exit planning. Availability of records in liquidation 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: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	Data Transfers (Cloud Data Processing Addendum) N/A Intellectual Property Data Export (Cloud Data Processing Addendum) Term and Termination

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
83	b) The governing law of the arrangement shall also be clearly specified. In principle, arrangements shall only be entered into with parties operating in jurisdictions upholding confidentiality clauses and agreements.	Refer to your Google Cloud Financial Services Contract.	Governing Law
84	c) The right of the RE and the RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction shall be ensured.	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
85	d) The arrangement shall comply 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
86	**Chapter – X Exit Strategy**		
87	22. **Exit Strategy**		
88	a) The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy, the RE shall, *inter alia*, identify alternative arrangements, which may include performing the activity by a different service provider or RE itself.	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. 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. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information. 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:	Data Export (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		-Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. -Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. -Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Engaging in dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	
89	b) REs shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the RE and new service provider(s) to ensure there is a smooth transition. Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised by the regulator/ concerned RE.	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. 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.	Deletion on Termination (Cloud Data Processing Addendum) Transition Term Transition Assistance

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
90	**Appendix – I Usage of Cloud Computing Services**		
91	There are several cloud deployment and service models that have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. Each of these models come with corresponding service, business benefit and risk profiles.	Google Cloud is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy Google Cloud as part of a hybrid or multi-cloud deployment.	N/A
92	In addition to the Outsourcing of IT Services controls prescribed in these Directions, REs shall adopt the following requirements for storage, computing and movement of data in cloud environments:		
93	1. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A
94	2. In engaging cloud services, REs shall ensure, *inter alia*, that the Outsourcing of IT Services policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The REs shall ensure that the procedures specified 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. 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 Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud.	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
95	3. In adoption of cloud services, REs shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the RE and the Cloud Service Provider (CSP). REs may refer to some of the *cloud security best practices*, for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.	This is addressed in the Cloud Data Processing Addendum. 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. Google publishes a number of resources to help customers understand how to configure robust security for our services: • Security best practices • Security use cases • Security blueprints	N/A
96	4. **Cloud Governance**: REs shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, *inter alia*, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage	Refer to Rows 90 to 124.	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.		
97	5. **Cloud Service Providers (CSP)**		
98	**Considerations for selection of CSP**: REs shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. REs shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to REs, 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
		.	
99	6. **Cloud Services Management and Security Considerations**		
100	a) **Service and Technology Architecture:** REs shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. REs shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the RE. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture should 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.	Cloud infrastructure resilience Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper 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.	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
101	b) **Identity and Access Management (IAM):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented 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 against 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.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **Multi-Factor Authentication** provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with Google Cloud whitepaper explains Google's data access processes and policies. 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)
102	c) **Security Controls**: REs shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise 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 RE; necessary procedures to authorise changes to cloud applications and related resources.	Security controls Refer to Row 14 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 Identity Security? blog post. 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.	Data Security; Google's Security Measures (Cloud Data Processing Addendum) Access and Site Controls (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic 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 against 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. 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.	

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
103	d) **Robust Monitoring and Surveillance:** REs shall accurately define minimum monitoring requirements in the cloud environment. REs should ensure to assess the information/ cyber security capability of the cloud service provider, such that the:	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
104	i) CSP 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 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.	N/A
105	ii) CSP 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.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
106	iii) nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the RE 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) • PCI DSS You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Customer Penetration Testing Certifications and Audit Reports
107	iv) CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, 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.	Google Subcontractors Data Security; Access and Compliance (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
108	e) Appropriate integration of logs, events from the CSP into the RE's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured 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 in our Data incident response whitepaper. 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. Our Autonomic Security Operations (ASO) solution: ● 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: ● Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. ● Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment.	Data Incidents (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	
109	f) The RE's own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / RE shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/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. In your Google Cloud environment, you can use Chronicle and VirusTotal to monitor and respond to many types of malware. -Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with Chronicle. -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	N/A

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
110	g) Vulnerability Management: REs shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.	Refer to Rows 103 to 109.	N/A
111	7. **Disaster Recovery & Cyber Resilience**		
112	a) The RE's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the RE can continue its critical operations with minimal disruption of services while ensuring 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. • Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on GCP across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit.	Data Export (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 our commitment to open source and common standards.	
113	b) REs shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured, *inter alia*, through robust incident response and recovery practices including conduct of Disaster Recovery (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 this blog post for more information about the resilience testing that Google performs as well as recommendations on how to train your first responders so they can react efficiently under pressure. You'll also find templates so you can get started testing these methods in your own organization. Firms can also request to review Google Cloud's testing results.	Business Continuity and Disaster Recovery
114	8. The following points may be evaluated while developing an exit strategy:		
115	a) the exit strategy and service level stipulations in the SLA shall factor in, *inter alia,*	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 Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos	Data Export (Cloud Data Processing Addendum)

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud. 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. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page.	
116	i) agreed processes and turnaround times for returning the RE's service collaterals and data held by the CSP;	Refer to Row 115.	N/A
117	ii) data completeness and portability;	Refer to Row 115.	N/A
118	iii) secure purge of RE's information from the CSP's environment;	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)
119	iv) smooth transition of services; and	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.	Transition Term
120	v) unambiguous definition of liabilities, damages, penalties and indemnities.	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.	Services

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Liability Indemnification
121	b) monitoring the ongoing design of applications and service delivery technology stack that the exit plans should align with.	Refer to Row 102 on configuration management and monitoring.	N/A
122	c) contractually agreed exit / termination plans should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the RE's business, while maintaining integrity and security.	Refer to Row 119 on the transition term that Google provides. 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
123	d) All records of transactions, customer and operational information, configuration data should be promptly taken over in a systematic manner from the CSP and purged at the CSP-end and independent assurance sought 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)
124	9. **Audit and Assurance:** The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, *inter alia*, aspects such as roles and responsibilities of both RE 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, etc.	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. Certifications and Audit Reports

Reserve Bank of India - Master Direction on Outsourcing of Information Technology Services 2023

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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: • 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.	