RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

This document is designed to help banks supervised by the Reserve Bank of India ("**regulated entity**") to consider the Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks (the "**framework**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Section 5.4 (Evaluating the Capability of the Service Provider) Section 5.5 (The Outsourcing Agreement), Section 5.6 (Confidentiality and Security), Section 5.8 (Business Continuity and Management of Disaster Recovery Plan), Section 5.9 (Monitoring and Control of Outsourced Activities) and and Section 7 (Off-shore outsourcing of Financial 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.	5.4	**Evaluating the Capability of the Service Provider**		
2.	5.4.1	In considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational and reputational factors. Banks should consider whether the service providers' systems are compatible with their own and also whether their standards of performance including in the area of customer service are acceptable to it. Banks should also consider, while evaluating the capability of the service provider, issues relating to undue concentration of outsourcing arrangements with a single service provider. Where possible, the bank should obtain independent reviews and market feedback on the service provider to supplement its own findings.	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 for each of the areas you need to consider below and in the rows that follow. Compatibility There are a number of ways to integrate our services with your systems. • Google Workspace Marketplace API allows you to access a repository of Google Workspace APIs in a centralised location for easy integration. • Google Workspace also enables you to integrate with reliable third-party business solutions. More information is available on our Partner Integration page. Standards of performance The SLAs provide measurable performance standards for the services and are available on our Google Workspace Service Level Agreement. 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.	N/A Services N/A

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
3.	5.4.2 Due diligence should involve an evaluation of all available information about the service provider, including but not limited to:-		
4.	• Past experience and competence to implement and support the proposed activity over the contracted period;	Qualifications and competencies: 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. Principals: Information about Google Cloud's leadership team is available on our Media Resources page. Customer references: Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Cloud Customer page	N/A
5.	• Financial soundness and ability to service commitments even under adverse conditions;	You can review information about Google's financial condition on Alphabet's Investor Relations page.	N/A
6.	• Business reputation and culture, compliance, complaints and outstanding or potential litigation;	Reputation For more information on Google's business reputation, refer to Row 4. 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 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	N/A N/A Representation and Warranties

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Information about material pending legal proceedings is available in our annual reports page	N/A
7.	• Security and internal control, audit coverage, reporting and monitoring environment, Business continuity management;	Security and internal controls and audit coverage Google recognizes that regulated entities need to review our internal controls, systems and data security and privacy protections for the services as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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) • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The Status Dashboard provides status information on the Services.	Certifications and Audit Reports Ongoing Performance Monitoring

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). Reporting 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 Status 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. 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. Information on the reliability of the Services is available on our Google Cloud Help page.	Significant Developments Data Incidents (Data Processing Amendment) Business Continuity and Disaster Recovery

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
8.	• External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact 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 is available here. • Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. 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 Trusting your data with G Suite whitepaper	Data Transfers (Data Processing Amendment) Data Security; Subprocessors (Data Processing Amendment) Data Transfers (Data Processing Amendment)
9.	• Ensuring due diligence by service provider of its employees.	Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees.	N/A
10.	5.5 **The Outsourcing Agreement**		
11.	5.5.1 The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by bank's legal counsel on their legal effect and enforceability. Every such agreement should address the risks and risk mitigation strategies. The agreement should be sufficiently flexible to allow the bank to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement should also bring out the nature of legal relationship between the parties – i.e.	The terms and conditions governing the relationship between the parties are set out in the Google Cloud Financial Services Contract.	N/A

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	whether agent, principal or otherwise. Some of the key provisions of the contract would be:		
12.	• The contract should clearly define what activities are going to be outsourced including appropriate service and performance standards.	The Google Workspace services are described on our services summary page. The SLAs are available on our Google Workspace Service Level Agreement page	Definitions Services
13.	• The bank must ensure it has the ability to access all books, records and information relevant to the outsourced activity available with the service provider.	Google grants audit, access and information rights to regulated entities. Regulated entities may access their data on the services at any time	Customer Information, Audit and Access
14.	• The contract should provide for continuous monitoring and assessment by the bank of the service provider 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 more information, refer to Row 7.	Ongoing Performance Monitoring
15.	• A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included.	You 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 may terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
16.	• Controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.	Confidentiality This is addressed in the Data Processing Amendment where Google makes commitments to protect your data, including regarding security. For more information about the security of our services, refer to Row 26. Liability Refer to your Google Cloud Financial Services Contract.	Confidentiality Data Security; Security Measures (Data Processing Amendment) Liability

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
17.	• Contingency plans to ensure business continuity.	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. Information on the reliability of the Services is available on our Google Cloud Help page.	Business Continuity and Disaster Recovery
18.	• The contract should provide for the prior approval/consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity.	Google recognizes that regulated entities need to consider the risks associated with sub-contracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. To enable regulated entities to retain oversight of any sub-outsourcing 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
19.	• Provide the bank with the right to conduct audits on the service provider 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 on the service provider in conjunction with the services performed for the bank.	Audit right Google recognizes that regulated entities must be able to audit our services effectively. 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. Audit reports	Customer Information, Audit and Access

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. For more information on the third-party audit reports that Google provides refer to Row 7.	Certifications and Audit Reports
20.	• Outsourcing agreements should include clauses to allow the Reserve Bank of India or persons authorised by it to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time.	Google grants audit, access and information rights to supervisory authorities and their appointees. Regulated entities can access their data on the service at any time and provide their supervisory authorities with access.	Regulator Information, Audit and Access Customer Information, Audit and Access
21.	• Outsourcing agreement should also include clause to recognise the right of the Reserve Bank to cause an inspection to be made of a service provider of a bank and its books and account by one or more of its officers or employees or other persons.	See above.	N/A
22.	• In cases where the controlling/Head offices of foreign banks operating in India outsource the activities related to the Indian operations, the Agreement should include clauses to allow the RBI or persons authorized by it to access the bank's documents, records of transactions and other necessary information given or stored or processed by the service provider within a reasonable time as also clauses to recognise the right of RBI to cause an inspection to be made of a service provider and its books and accounts by one or more of its officers or employees or other persons.	See above. The supervisory authority's audit, access and information rights apply regardless of the service location.	Regulator Information, Audit and Access
23.	• The outsourcing agreement should also provide that confidentiality of customer's information should be maintained even after the contract expires or gets terminated.	Google's commitments to protect customer data in the Data Processing Amendment remain in effect until the data is deleted. In addition, Google's confidentiality obligations survive expiry or termination of the contract.	Duration (Data Processing Amendment) Survival

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24.	• The outsourcing agreement should provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard.	Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Data Deletion (Data Processing Amendment)
25.	5.6 **Confidentiality and Security**		
26.	5.6.1 Public confidence and customer trust in the bank is a prerequisite for the stability and reputation of the bank. Hence the bank should seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.	The confidentiality and security of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page (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.	Confidentiality Data Security; Security Measures (Data Processing Amendment)

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(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 certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases	

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	5.6.2	Access to customer information by staff of the service provider should be on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. In particular, Google Workspace Audit Logs help your security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events.	N/A
28.	5.6.3	The bank should ensure that the service provider is able to isolate and clearly identify the bank's customer information, documents, records and assets to protect the confidentiality of the information. In instances, where service provider acts as an outsourcing agent for multiple banks, care should be taken to build strong safeguards so that there is no comingling of information/documents, records and assets.	To keep data private and secure, Google logically isolates each customer's data from that of other customers. Refer to Row 26 for more information on Google's security measures.	Security Measures; Data Storage, Isolation and Logging (Data Processing Amendment)
29.	5.6.4	The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.	Security practices For more information on security practices and control processes, refer to Row 26. Security breaches 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.	N/A Data Incidents (Data Processing Amendment)
30.	5.6.5	The bank should immediately notify RBI in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the bank would be liable to its customers for any damage.	See above.	N/A
31.	5.8	**Business Continuity and Management of Disaster Recovery Plan**		

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
32.	5.8.1	A bank should require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Banks need to ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service provider.	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. Information on the reliability of the Services is available on our Google Cloud Help page.	Business Continuity and Disaster Recovery
33.	5.8.2	In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, banks should retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the bank and its services to the customers.	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. Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page. In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.	Transition Term Data Export (Data Processing Amendment)
34.	5.8.3	In establishing a viable contingency plan, banks should 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.	Refer to Row 33 for more information about how you can retrieve your data from the services. Regulated entities can use Spinbackup as part of their backup routine. Refer to our solutions page for more information about how you can configure Spinbackup Google Workspace backup and restore your Google Workspace data.	N/A
35.	5.8.4	Outsourcing often leads to the sharing of facilities operated by the service provider. The bank should ensure that service providers are able to isolate the	To keep data private and secure, Google logically isolates each customer's data from that of other customers. For more information on Google's security, refer to Row 26.	N/A

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		bank's information, documents and records, and other assets. This is to ensure that in adverse conditions, all documents, records of transactions and information given to the service provider, and assets of the bank, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.	For more information on how you can retrieve your data, refer to Row 33.	
36.	5.9	**Monitoring and Control of Outsourced Activities**		
37.	5.9.1	The bank should have in place a management structure to monitor and control its outsourcing activities. It should ensure that outsourcing agreements with the service provider contain provisions to address their monitoring and control of outsourced activities.	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. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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
38.	5.9.2	A central record of all material outsourcing that is readily accessible for review by the Board and senior management of the bank should be maintained. The records should be updated promptly and half yearly reviews should be placed before the Board.	This is a customer consideration.	N/A
39.	5.9.3	Regular audits by either the internal auditors or external auditors of the bank should assess the adequacy of the risk management practices adopted in	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	Customer Information, Audit and Access

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework and the requirements of these guidelines.	auditor appointed by the regulated entity.	
40.	5.9.4	Banks should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity 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 Data incident response whitepaper. For more information on due diligence reviews, refer to Rows 2 to 9.	Significant Developments
41.	5.9.5	In the event of termination of the agreement for any reason, this should be publicized so as to ensure that the customers do not continue to entertain the service provider.	This is a customer consideration.	N/A
42.	7	**Off-shore outsourcing of Financial Services**		
43.	7.1	The engagement of service providers in a foreign country exposes a bank to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the bank. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the bank. To manage the country risk involved in such outsourcing activities, the bank should take into account and closely monitor government policies and political, social, economic and legal conditions in countries where the service provider is based, during the risk assessment process and on a continuous basis, and establish sound procedures for dealing with country risk problems. This includes having appropriate contingency and exit strategies. In principle, arrangements should only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement should also be clearly specified.	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 is available here. • Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region.	Data Transfers (Data Processing Amendment) Data Security; Subprocessors Data Processing Amendment)

RBI - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

Google Workspace Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 Trusting your data with G Suite whitepaper. Governing Law Refer to your Google Cloud Financial Services Contract.	Data Transfers (Data Processing Amendment) Governing Law
44.	7.2 The activities outsourced outside India should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of the bank in a timely manner.	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights regardless of the service location.	Enabling Customer Compliance
45.	7.3 The outsourcing related to overseas operations of Indian banks would be governed by both, these guidelines and the host country guidelines. Where there are differences, the more stringent of the two would prevail. However where there is any conflict, the host country guidelines would prevail.	You can review information about how Google addresses global outsourcing requirements at our Google Cloud Compliance Resource Center.	N/A