



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

This document is designed to help insurers supervised by the Insurance Regulatory and Development Authority of India (“**regulated entity**”) to consider the [Outsourcing of Activities by Indian Insurers Regulations, 2017](#) (“**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: Section 10 (Due Diligence of Outsourcing Service Providers), Section 11 (Outsourcing Agreements), Section 12 (Confidentiality and Security), Section 13 (Inspection and Audit by the Insurer), Section 14 (Legal and Regulatory Obligations), Section 16 (Contingency Plans), Section 18 (Regulatory Access). 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.	10. DUE DILIGENCE OF OUTSOURCING SERVICE PROVIDERS		
2.	Among other things, an outsourcing arrangement shall be considered material if the estimated annual expenditure under an outsourcing contract is likely to exceed 5 % of the total expenditure incurred during preceding financial year on all outsourcing activities. All insurers shall evaluate the outsourcing arrangements based on the detailed parameters for materiality assessment outlined in Annexure I.	This is a customer consideration.	N/A
3.	All outsourcing arrangements assessed as material shall be subject to evaluation of the risks envisaged under Annexure II and shall be subject to due diligence as per (i) &(ii) below. Insurers should consider the level of materiality associated with their outsourced activities and implement their enterprise risk management practices deemed as appropriate to the specific nature and circumstances of activities.	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	N/A
4.	i. In considering or renewing an outsourcing arrangement, an insurer should subject the outsourcing service provider to appropriate due diligence which inter alia cover the following;		
5.	a) Where the outsourcing service provider is a Company registered under the Companies Act, 2013, the objects of the Memorandum of Association of the company shall include the activities outsourced.	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
6.	b) In case of other outsourcing service provider, there shall be a clause in the deeds or bye laws enabling it to undertake the activities outsourced.	Refer to Row 6 above.	N/A
7.	c) Existence of the outsourcing service provider as projected, its competence and experience to perform the activity proposed to be outsourced to it.	<u>Competence</u> <ul style="list-style-type: none">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. <u>Experience</u> <ul style="list-style-type: none">Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science,	N/A



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page.	
8.	d) Assessing the capability of the outsourcing Service Provider to employ standards envisaged, while performing outsourced activities.	<p><u>Service levels</u></p> <p>The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements.</p> <p><u>Assessing performance</u></p> <p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <ul style="list-style-type: none">• 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).	<p>Services</p> <p>Ongoing Performance Monitoring</p>
9.	e) Its security and internal controls;	<p><u>Security</u></p> <p>Refer to Row 24 for information on Google's security practices.</p> <p><u>Internal controls</u></p> <p>Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p>	<p>N/A</p> <p>Certifications and Audit Reports</p>



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">ISO/IEC 27001:2013 (Information Security Management Systems)ISO/IEC 27017:2015 (Cloud Security)ISO/IEC 27018:2014 (Cloud Privacy)PCI DSSSOC 1SOC 2SOC 3 <p>You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.</p>	
10.	f) Business continuity management;	<p>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.</p> <p>In addition, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications.</p>	Business Continuity and Disaster Recovery
11.	g) Where considered necessary, insurers shall obtain independent reviews and market feedback on the service provider to supplement its own findings;	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.	N/A
12.	ii. Due diligence undertaken during the selection process should be documented and evaluated at least annually as part of the monitoring and control process of outsourcing.	This is a customer consideration.	N/A
13.	iii. The due diligence may be as specified in the Board approved Outsourcing Policy as per Regulation 7(i)(f) for activities other than material.	This is a customer consideration.	N/A
14.	11. OUTSOURCING AGREEMENTS		
15.	i. Outsourcing arrangements shall be governed by written agreements that are legally binding for a specified period, subject to periodical renewals, if necessary, that clearly describe all important aspects of the outsourcing arrangement, including the rights and obligations of all parties.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
16.	ii. The outsourcing contracts, inter alia, shall have in place certain clauses or conditions listed below, as may be applicable:		
17.	a) Information and asset ownership rights, information technology, data security and protection of confidential information	<p><u>Ownership</u></p> <p>You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination.</p> <p><u>Security</u></p> <p>Refer to Row 24 for more information on Google's security practices.</p> <p><u>Confidentiality</u></p> <p>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.</p>	<p>Intellectual Property</p> <p>N/A</p> <p>Confidentiality</p>
18.	b) Guarantee or indemnity from the outsourcing service provider towards his commitment including liability for any failure	Refer to your Google Cloud Financial Services Contract.	Indemnification
19.	c) Contingency planning of the outsourcing service Provider to provide business continuity for the outsourced arrangements that are material	<p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p>	Business Continuity and Disaster Recovery
20.	d) Express clause that the contract shall neither prevent nor impede Insurer from meeting its respective regulatory obligations, nor the IRDAI from exercising its regulatory powers of conducting inspection, investigation, obtaining information from either the Insurer or the outsourcing service provider	<p>Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.</p> <p>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.</p>	Enabling Customer Compliance
21.	e) Contract termination clause specifying orderly handing over of data, assets etc.	<p><u>Termination</u></p> <p>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.</p>	Term and Termination



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.</p> <p><u>Transfer</u></p> <p>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:</p> <ul style="list-style-type: none">• 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 here and on storage options here. <p><u>Deletion</u></p> <p>On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.</p>	<p>Data Export (Cloud Data Processing Addendum)</p> <p>Deletion on Termination (Cloud Data Processing Addendum)</p>
22.	iii. The Insurer shall ensure that the outsourcing service provider shall not sub-contract the whole or a substantial portion of the Outsourced activity. Where sub-contracting is allowed partially it should be with the prior consent of the Insurer and the additional risk which flows due to subcontracting shall be factored in at the time of due diligence.	<p>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.</p> <p>To enable regulated entities to retain oversight of any sub-outsourcing and provide choices about the services they use, Google will:</p> <ul style="list-style-type: none">• provide information about our subcontractors;• provide advance notice of changes to our subcontractors; and• give regulated entities the ability to terminate if they have concerns about a new subcontractor. <p>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.</p>	Subcontracting; Google Subcontractors



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

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.	
23.	12. CONFIDENTIALITY AND SECURITY		
24.	i. The insurer shall satisfy itself that the outsourcing service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of policyholders' information even after the contract terminates.	<p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Google's commitments to protect customer data in the Cloud Data Processing Addendum remain in effect until the data is deleted.</p> <p>The confidentiality and security of a cloud service consists of two key elements:</p> <p><u>(1) Security of Google's infrastructure</u></p> <p>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p> <p>Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis.</p> <p>More information is available at:</p> <ul style="list-style-type: none">• Our infrastructure security page• Our security whitepaper• Our cloud-native security whitepaper• Our infrastructure security design overview page• Our security resources page <p>In addition, you can review Google's SOC 2 report.</p> <p><u>(2) Security of your data and applications in the cloud</u></p> <p>You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services.</p>	<p>Confidentiality</p> <p>Data Security; Security Measures (Cloud Data Processing Addendum)</p>



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>(a) <u>Security by default</u></p> <p>Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you:</p> <ul style="list-style-type: none">• <u>Encryption at rest</u>. 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.• <u>Encryption in transit</u>. 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. <p>(b) <u>Security products</u></p> <p>In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page.</p> <p>(c) <u>Security resources</u></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none">• Security best practices• Security use cases• Security blueprints	
25.	ii. It shall be the responsibility of the insurer to ensure that the data or information parted to any outsourcing service provider under the outsourcing agreements remains confidential.	Refer to Row 24 for more information on how Google keeps your data confidential.	N/A
26.	iii. An insurer shall take into account any legal or contractual obligations on the part of the outsourcing service provider to disclose the outsourcing arrangement and circumstances under which Insurer's customer data may be disclosed. In the event of termination of the outsourcing agreement, the insurer should ensure that	<p><u>Protection from disclosure</u></p> <p>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.</p>	Confidentiality



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	the customer data is retrieved from the service provider and ensure there is no further use of customer data by the service provider.	<p>Google understands that this is important and is committed to maintaining trust with customers by being transparent about how we respond to government requests.</p> <p>If Google receives a government request, Google will:</p> <ul style="list-style-type: none">• attempt to redirect the request to the customer• notify the customer prior to disclosure unless prohibited by law• comply with the customer requests to oppose disclosure• only disclose if strictly necessary to comply with legal process <p>More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper.</p> <p>To provide even more transparency, Google reports the government requests we receive for enterprise Cloud customers in our Enterprise Cloud Transparency Report.</p> <p><u>Retrieval</u></p> <p>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:</p> <ul style="list-style-type: none">• 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 here and on storage options here. <p><u>Deletion on termination</u></p> <p>On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.</p>	<p>Data Export (Cloud Data Processing Addendum)</p> <p>Deletion on Termination (Cloud Data Processing Addendum)</p>



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	13. INSPECTION AND AUDIT BY THE INSURER		
28.	The insurer shall conduct periodic inspection or audit on the outsourcing service providers either by internal auditors or by Chartered Accountant firms appointed by the insurer to examine the compliance of the outsourcing agreement while carrying out the activities outsourced.	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 the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.	Regulator Information, Audit and Access Customer Information, Audit and Access
29.	The outsourcing committee of the Insurer may decide on the periodicity and service providers to be inspected taking into account the risks associated with the activity outsourced. Insurer shall ensure that enabling provisions for the Inspection by the Insurer shall be included in the Agreement with outsourcing service provider. Measures shall be taken to arrest the deficiencies noticed if any in the inspection or audit report.	<u>Audit frequency and scope</u> 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. <u>Remediation</u> Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls.	Customer Information, Audit and Access N/A
30.	14. LEGAL AND REGULATORY OBLIGATIONS		
31.	i. Insurers shall ensure that outsourcing arrangements do not,		
32.	a) diminish their ability to fulfil their obligations to Policyholders and the IRDAI	Google recognizes that using our Services should not impair a regulated entity's ability to oversee compliance with applicable laws and regulations as well as a regulated entity's internal policies. We will provide regulated entities with the assistance they need to review our Services.	Enabling Customer Compliance
33.	b) impede effective supervision by the IRDAI	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.	Enabling Customer Compliance
34.	c) result in their internal control, business conduct or reputation being compromised or weakened	Refer to Row 24 for information on Google's security practices. Refer to Row 9 for information about the third party certifications and audit reports that Google maintains.	N/A
35.	ii. The Regulations apply irrespective of whether the outsourcing arrangements are entered into with an affiliated entity within the same group as the Insurer, or an outsourcing service Provider external to the group or the one who has been given sub-contract	This is a customer consideration.	N/A



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
36.	iii. Outsourcing shall not diminish the obligations of an insurer and those of its Board and Senior Management to comply with the relevant law/s and regulations. The Insurer is ultimately accountable for all acts of commission and omission of the outsourcing service providers. The Insurer's liability shall not in any way be restricted or limited by way of outsourcing.	This is a customer consideration.	N/A
37.	iv. All the outsourcing service providers engaged by insurers are subject to the provisions of the Insurance Act, 1938, IRDA Act 1999, Rules, Regulations and any other orders issued thereunder.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
38.	v. The regulated activities of the Insurance Agents, Insurance Intermediaries including TPAs, Insurance Repositories and other regulated entities, as provided in the Insurance Act, 1938, IRDA Act 1999 and Regulations, guidelines made thereunder are not considered as outsourcing and therefore not covered by these Regulations.	This is a customer consideration.	N/A
39.	vi. Subject to these Regulations, Insurance Agents, Insurance Intermediaries and other regulated entities of the Authority shall not be contracted for performing any activity other than those activities that are allowed under the respective regulations or guidelines notified by the Authority from time to time governing their registration or functioning.	This is a customer consideration.	N/A
40.	a) Provided these provisions are not applicable in respect of entities regulated by RBI and Post Offices when they are engaged for premium collection and cheque pick-up activities.	This is a customer consideration.	N/A
41.	b) Provided also that these provisions are not applicable to Insurer involving Senior Agents as faculty in the training sessions purely on honorarium basis.	This is a customer consideration.	N/A
42.	c) Provided also that the services allowed to be outsourced to registered Insurance Repositories or other regulated entities by the respective regulations or guidelines will be governed by these regulations.	This is a customer consideration.	N/A
43.	vii. The Authority may issue guidelines with regard to permitting or restricting outsourcing of specific activities to certain categories of unregulated entities.	Google appreciates 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
44.	16. CONTINGENCY PLANS		
45.	i. Insurers shall establish and maintain adequate contingency plans where the outsourced activity is material. These include disaster recovery plans and backup facilities to support the continuation of an outsourced activity with minimal	<u>Contingency plans</u>	Business Continuity and Disaster Recovery



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	business disruption in the event of reasonably foreseeable events that affect the ability of an outsourcing service provider to continue providing the service.	<p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> <p><u>Back-up</u></p> <p>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.</p>	
46.	ii. The contingency plans should be appropriate to the potential consequences of a business disruption resulting from problems at the outsourcing service provider and should consider contingency plans maintained by the outsourcing service provider and their coordination with the Insurer's own contingency arrangements. In particular, contingency plans should ensure that the Insurer can readily access all the records necessary to allow it to sustain business operations, meet statutory obligations, and provide any information relating to the outsourced activity as may be required by the IRDAI.	<p><u>Exit planning</u></p> <p>We recognize 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.</p> <p>We support such exit plans through:</p> <ul style="list-style-type: none">• 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. <p>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 commit to open source and common standards.</p> <p><u>Data access</u></p>	<p>Data Export (Cloud Data Processing Addendum)</p> <p>Data Export (Cloud Data Processing Addendum)</p>



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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:</p> <ul style="list-style-type: none">• 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 here and on storage options here. <p>Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.</p>	Regulator Information, Audit and Access
47.	iii. Contingency plans should also be regularly reviewed and tested to ensure that they remain robust, particularly under changing operating conditions.	Refer to Row 45 for information on Google's approach to contingency planning.	N/A
48.	18. REGULATORY ACCESS		
49.	i. Insurers shall, in all cases, obtain an undertaking from their outsourcing Service providers or include a provision within the outsourcing agreement, giving authorized representatives of the IRDAI the right to:-		
50.	a) examine the books, records, information, systems and the internal control environment in the outsourcing service provider (or sub-contractor as applicable), to the extent that they relate to the service being performed for the Insurer and	<p>Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.</p> <p>Google recognizes that chain-outsourcing 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.</p>	Regulator Information, Audit and Access Customer Information, Audit and Access Google Subcontractors
51.	b) access any internal audit reports or external audit findings of the outsourcing service Provider that concern the service being performed for the Insurer.	<p>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:</p> <ul style="list-style-type: none">• ISO/IEC 27001:2013 (Information Security Management Systems)• ISO/IEC 27017:2015 (Cloud Security)	Certifications and Audit Reports



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none">ISO/IEC 27018:2014 (Cloud Privacy)PCI DSSSOC 1SOC 2SOC 3 <p>You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.</p>	
52.	ii. In cases where Insurer outsources to the service providers outside India, the Insurers shall ensure that the terms of the agreement are in compliance with respective local regulations governing the outsourcing service provider and laws of the country concerned and such laws and regulations do not impede the regulatory access and oversight by the Authority. All original policyholder records continue to be maintained in India.	<p><u>Location</u></p> <p>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.</p> <ul style="list-style-type: none">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. <p>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:</p> <ul style="list-style-type: none">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. <p>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).</p> <p>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.</p> <p><u>Regulatory access and oversight</u></p> <p>Google recognizes that regulated entities and their supervisory authorities must be able</p>	<p>Data Transfers (Cloud Data Processing Addendum)</p> <p>Data Security; Subprocessors (Cloud Data Processing Addendum)</p> <p>Data Location (Service Specific Terms)</p> <p>Regulator Information, Audit and Access</p>



IRDAI - Outsourcing of Activities by Indian Insurers Regulations, 2017

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Customer Information, Audit and Access