HKIA - Outsourcing GL14

Google Cloud Mapping

This document is designed to help authorised insurers supervised by the Hong Kong Insurance Authority ("**regulated entity**") to consider the GL14 Guideline on Outsourcing ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on paragraphs 5.8 to 5.21 of the framework, which covers the following areas: Service Provider, Outsourcing Agreement, Monitoring and Control, Contingency Planning, Overseas outsourcing and Subcontracting. 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.	**Service Provider**		
2.	5.8. An authorized insurer should exercise due diligence and care and consider factors such as aggregate exposure to that particular service provider, possible conflict of interest that may arise, and price of the outsourcing vis-à-vis the benefit gained in assessing and selecting a service provider. Besides, when assessing a service provider, it should, among other things, take into account the following factors of the service provider:	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 information for each of the areas you need to consider in the rows that follow.	N/A
3.	(a) reputation, experience and quality of service;	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
4.	(b) financial soundness, in particular, the ability to continue to provide the expected level of service;	You can review information about Google's financial condition on Alphabet's Investor Relations page.	N/A
5.	(c) managerial skills, technical and operational expertise and competence, in particular, the ability to deal with disruptions in business continuity;	Information about Google Cloud's leadership team is available on our Media Resources page. Refer to Rows 43 to 48 on contingency planning.	N/A
6.	(d) any licence, registration, permission or authorization required by law to perform the outsourced service;	Google will comply with all laws and regulations applicable to it in the provision of the Services.	Representations and Warranties
7.	(e) extent of reliance on sub-contractors and effectiveness in monitoring the work of sub-contractors;	Refer to Rows 57 to 59 on sub-contracting.	N/A
8.	(f) compatibility with the insurer's corporate culture and future development strategies; and	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.	N/A
9.	(g) familiarity with the insurance industry and capacity to keep pace with innovation in the market.	Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page.	N/A
10.	5.9. An authorized insurer should periodically review (at least annually) the ability (including financial strength and technical competence) of the selected service provider to ascertain whether it can continue to provide the expected level of service.	This is a customer consideration.	N/A
11.	**Outsourcing Agreement**		

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
12.	5.10. An outsourcing arrangement should be undertaken in the form of a legally binding written agreement. In negotiating the contract with the service provider, an authorized insurer should consider, among other things, the following matters:	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
13.	(a) scope of the outsourced service;	The GCP services are described on our services summary page.	Definitions
14.	(b) location where the outsourced service will be performed;	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. • Google makes the same commitments about all its subprocessors, regardless of country / region.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)
15.	(c) effective period of the outsourcing arrangement;	Refer to your Google Cloud Financial Services Contract	Term and Termination
16.	(d) contractual obligations and liabilities of the insurer and the service provider;	Refer to your Google Cloud Financial Services Contract	Liability
17.	(e) performance standards to be attained in respect of the outsourced service. This is particularly appropriate when the insurer has committed a service standard or performance pledge to its customers;	The SLAs are available on our Google Cloud Platform Service Level Agreements page	Services
18.	(f) reporting or notification requirements that the insurer may wish to impose on the service provider;	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. 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)

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
19.	(g) the way in which the insurer and the service provider should monitor the performance under the agreement (e.g. evaluation of performance through service delivery reports, periodic self-certification, independent reviews by the insurer's or service provider's auditors);	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). Independent reviews 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	Ongoing Performance Management Certifications and Audit Reports
20.	(h) information and asset ownership rights, information technology security and protection of confidential information;	Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Security The security of a cloud service consists of two key elements: Security of Google's infrastructure	Intellectual Property

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 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 at: https://cloud.google.com/security/encryption-at-rest/default-encryption. ● **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 at https://cloud.google.com/security/encryption-in-transit. (b) Security products	Data Security; Security Measures (Cloud Data Processing Addendum)

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
21.	(i) rules and restrictions on sub-contracting, e.g. requiring insurer's prior consent on sub-contracting of the outsourced service. The insurer should retain the ability to maintain similar control over its outsourcing risks when a service provider uses a sub-contractor;	Refer to Rows 57 to 59 on sub-contracting.	N/A
22.	(j) remedial action and escalation process for dealing with inadequate performance;	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
23.	(k) contingency planning of the service provider to provide business continuity for the outsourced service;	Refer to Rows 43 to 48 on contingency planning.	N/A
24.	(l) management and approval process for changes to the outsourcing arrangement;	Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period	Changes to Services
25.	(m) conditions under which the insurer or service provider can terminate the outsourcing agreement;	Institutions can elect to terminate our contract for convenience with advance notice, including if Google increases the fees or if necessary to comply with law. In addition, institutions may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency.	Term and Termination
26.	(n) termination agreement, including intellectual property and information rights and clarification of the process to ensure the smooth transfer of outsourced service either to another service provider or back to the insurer;	Refer to Row 34 on data retrieval.	N/A

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	(o) guarantee or indemnity from the service provider, e.g. an indemnity to the effect that any sub-contracting by the service provider of the outsourced service will be the responsibility of the service provider including liability for any failure on the part of the sub-contractor;	Refer to your Google Cloud Financial Services Contract.	Indemnification
28.	(p) requirement for the service provider to hold relevant insurance;	Google will maintain insurance cover against a number of identified risks.	Insurance
29.	(q) mechanism to resolve disputes that might arise under the outsourcing arrangement;	Refer to your Google Cloud Financial Services Contract	Governing Law
30.	(r) the service provider's agreement to allow access by the auditors and actuaries of the insurer and the IA to any books, records and information which facilitates them to discharge their statutory duties and obligations; and	Google grants audit, access and information rights to regulated entities, regulatory authorities and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
31.	(s) governing law of the outsourcing agreement. The agreement should preferably be governed by Hong Kong law.	Refer to your Google Cloud Financial Services Contract.	Governing Law
32.	5.11. Where the service provider is the head office or another branch of an authorized insurer, a memorandum of understanding which has been properly endorsed by its Board of Directors may be acceptable.	N/A	N/A
33.	5.12. An authorized insurer should ensure that the outsourcing arrangements comply with relevant laws and statutory requirements on customer confidentiality (e.g. the Personal Data (Privacy) Ordinance, Cap. 486 ("PDPO")). The insurer should ensure that it and the service provider have proper safeguards in place to protect the integrity and confidentiality of the insurer's information and customer data.	Google will comply with laws (including privacy laws) applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data in the Cloud Data Processing Addendum.	Representations and Warranties
34.	5.13. An authorized insurer should take into account any legal or contractual obligation to notify customers of the outsourcing arrangement and circumstances under which their data may be disclosed or lost. In the event of the termination of the outsourcing agreement, the insurer should ensure that all customer data are either retrieved from the service provider or destroyed.	Customer notification This is a customer consideration. Refer to Row 35 on the reporting and notifications Google provides to you. Retrieval Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). 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 during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:	Transition Term

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Deletion on Termination (Cloud Data Processing Addendum)
35.	5.14. An authorized insurer should notify the IA forthwith of any unauthorized access or breach of confidentiality by the service provider or its sub-contractor that affects the insurer or its customers.	Refer to Row 18 on the notifications Google provides. 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.	N/A
36.	**Monitoring and Control**		
37.	5.15. An authorized insurer should ensure that it has sufficient and appropriate resources to monitor and control the outsourcing arrangements at all times. For effective monitoring and control of the outsourcing arrangements, an authorized insurer should, among other things:		

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
38.	(a) ensure the responsibility for monitoring the service provider and the outsourced service to be assigned to staff with appropriate expertise;	This is a customer consideration	N/A
39.	(b) maintain a central list of the outsourcing arrangements that includes the name of each service provider, service outsourced, location where the outsourced service is performed, commencement date and expiry or renewal date of the outsourcing agreement, and contact details of the key persons of the service provider. The central list should also record similar information relating to any sub-contracting arrangement of the outsourced service;	Refer to Rows 14 and 15 on the location where the services are performed and key dates. In addition, refer to Rows 57 to 59 on the information Google provides about our subcontractors.	N/A
40.	(c) exercise due diligence and care to monitor each outsourcing arrangement to ensure the service is being delivered in the manner expected, and to ensure the provisions included in the outsourcing agreement are properly effected; and	Refer to Row 19 on how you can monitor Google's performance of the Services (including the SLAs).	N/A
41.	(d) conduct reviews or audits periodically (at least annually) to ensure that the outsourcing policy and the monitoring and control procedures are being effectively complied with.	Google grants audit, access and information rights to regulated entities and their appointees. In addition, refer to Row 19 on the independent reviews the services undergo.	Customer Information, Audit and Access
42.	5.16. Once an authorized insurer implements an outsourcing arrangement, it should regularly review the effectiveness and adequacy of its controls in monitoring the performance of the service provider and managing the risks associated with the outsourced service. The insurer should have reporting procedures that can promptly escalate problems relating to the outsourced service to the attention of the management of the insurer and the service provider. It should take appropriate rectification actions forthwith if deficiencies are identified. The insurer is expected to notify the IA forthwith of any significant problem that has the potential to materially affect its financial position, business operation or compliance with legal and regulatory requirements.	Refer to Row 19 on how you can monitor Google's performance of the Services and Row 18 on the notifications Google provides.	N/A
43.	**Contingency Planning**		
44.	5.17. An authorized insurer outsourcing service to a service provider should put in place a contingency plan to ensure that its business would not be disrupted as a result of undesired contingencies (e.g. systems failure) of the service provider. The following issues should be considered and properly addressed in formulating such contingency plan:	Information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide. In particular, as part of your contingency planning, you can choose to use Anthos 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

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
45.	(a) back-up facilities or availability of alternative service provider or possibility of bringing the outsourced service back in-house;	This is a customer consideration. Refer to Row 44 on how you can use the services in your business contingency planning.	N/A
46.	(b) procedures to be followed and the persons responsible for respective activities if business continuity problem arises; and	This is a customer consideration. Refer to Row 44 on how you can use the services in your business contingency planning.	N/A
47.	(c) procedures for regular reviews and testing of the contingency plan.	This is a customer consideration. Refer to Row 44 on how you can use the services in your business contingency planning.	N/A
48.	5.18. An authorized insurer should also ensure that the service provider has its own contingency plan in respect of daily operational and systems problems. The insurer should have adequate understanding of the service provider's contingency plan and consider the implications for its own contingency planning in the event that the outsourced service is interrupted due to undesired contingencies of the 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.	Business Continuity and Disaster Recovery
49.	**Overseas Outsourcing**		
50.	5.19. In addition to the essential issues mentioned above, an authorized insurer should pay particular attention to the following issues in relation to overseas outsourcing:		
51.	(a) Country risk – The country risks associated with overseas outsourcing should be taken into account. Such risks cover the social, economic and political conditions and the legal and regulatory systems of an overseas jurisdiction which may adversely affect the ability of the service provider to carry out the provisions of the outsourcing agreement and the ability of the insurer to effectively monitor the outsourced service and the service provider.	Refer to Row 14 on the locations where the services are performed. In addition, 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.	Location (Service Specific Terms)
52.	(b) Information confidentiality – There may be circumstances under which the insurer's information and customer data are subject to the right of access by an overseas authority (e.g. police and tax authority). The insurer should take into account the extent and possibility of such access right and, as considered appropriate, seek legal advice to clarify the position. In case an overseas authority seeks access to the insurer's customer data, the insurer should forthwith notify the IA.	Google understands that this is important and is committed to maintaining trust with customers by being transparent about how we respond to government requests. If Google receives a government request, Google will: ● 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	Confidentiality

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. To provide even more transparency, Google reports the government requests we receive for enterprise Cloud customers in our Enterprise Cloud Transparency Report.	
53.	(c) Notification to customers – Having regard to the additional risks posed by overseas outsourcing, the insurer should consider the need to inform their customers of the jurisdiction in which the service is to be performed and any right of access available to overseas authorities.	This is a customer consideration. Refer to Rows 51 and 52 on service location and lawful access.	N/A
54.	(d) Examination by the IA – The insurer should ensure that, although its service is outsourced to be performed outside Hong Kong, such arrangement would not, in any case, impede the ability of the IA to access in Hong Kong the books and records and other information of the insurer as necessary for the IA to carry out its statutory responsibilities.	Google grants audit, access and information rights to regulatory authorities and their appointees. These rights apply regardless of the service location.	Regulator Information, Audit and Access
55.	(e) Transfer of personal data – The insurer should pay particular attention to relevant provisions of PDPO if it needs to transfer personal data outside Hong Kong under an overseas outsourcing arrangement.	This is a customer consideration. Google makes commitments to protect your data, including regarding security, use, transfer, access and retention, in the Cloud Data Processing Addendum.	N/A
56.	(f) Governing law of agreement – The governing law of the outsourcing agreement should preferably be governed by Hong Kong law.	Refer to your Google Cloud Financial Services Contract.	Governing Law
57.	**Sub-contracting**		
58.	5.20. Additional risk will be posed on the risk profile of an authorized insurer if the service provider of the outsourcing arrangement is allowed to further contract the service out to other parties. The insurer should put in place adequate procedures to control and monitor such sub-contracting arrangements and ensure that the service provider will take into account the essential issues set out in this Guideline as if it was the insurer concerned when further contracting out the service.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. 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 ensure regulated entities retain oversight of any sub-contracting, Google will comply with clear conditions designed to provide transparency and choice.	Google Subcontractors
59.	5.21. An authorized insurer should incorporate in the outsourcing agreement rules and restrictions on sub-contracting, e.g. requiring insurer's prior consent for sub-contracting and making the service provider liable for the capability of the sub-contractor. The insurer should ensure that its service provider would not engage in sub-contracting arrangement which may impede its ability to carry out the provisions of the outsourcing agreement with the insurer, in	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 remain accountable to you for the performance of all subcontracted obligations. To enable regulated entities to retain oversight of any sub-outsourcing and provide choices about the services regulated entities use, Google will:	Google Subcontractors

HKIA - Outsourcing GL14

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	particular, the requirements on information confidentiality, contingency planning and information access right by regulator.	• 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 (including the audit and access rights).	