HKMA Outsourcing SA-2

Google Cloud Platform Mapping

This document is designed to help authorised institutions supervised by the Hong Kong Monetary Authority ("**regulated entities**") to consider the Guidance Note on Outsourcing SA-2 issued on 28 December 2001 ("**framework**") in the context of Google Cloud Platform and the Google Cloud Financial Services Contract.

We focus on Sections 2.3 to 2.9 of SA-2 of the framework. 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.	**2.3. Ability of Service Providers**		
2.	2.3.1. Before selecting a service provider AIs should perform appropriate due diligence. In assessing a provider, apart from the cost factor and quality of services AIs should take into account the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with the AI's corporate culture and future development strategies, familiarity with the banking industry and capacity to keep pace with innovation in the market.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below. Business background and strategy You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. Reputation • 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 Cloud Customer page. • Performance record: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard.	N/A
3.	2.3.2. AIs should have controls in place (e.g. comparison with target service level) to monitor the performance of service providers on a continuous basis.	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	Ongoing Performance Management

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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).	
4.	**2.4. Outsourcing Agreement**		
5.	2.4.1. The type and level of services to be provided and the contractual liabilities and obligations of the service provider should be clearly set out in a service agreement between AIs and their service provider.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. The GCP services are described on our services summary page. The SLAs are available on our Google Cloud Platform Service Level Agreements page	N/A Definitions Services
6.	2.4.2. AIs should regularly (e.g. annually) review their outsourcing agreements. They should assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies.	This is a customer consideration.	N/A
7.	2.4.3 Where the service provider is a wholly-owned subsidiary of an AI or the head office or another branch of a foreign AI, a memorandum of understanding may be acceptable.	N/A	N/A
8.	**2.5. Customer Data Confidentiality**		
9.	2.5.1. AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. the Personal Data (Privacy) Ordinance – ("PDPO") and common law customer confidentiality. This will generally involve seeking legal advice.	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 Data Processing and Security Terms.	Representations and Warranties

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
10.	2.5.2. AIs should have controls in place to ensure that the requirements of customer data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of customer information. Typical safeguards include, among other things:	The confidentiality and integrity of a cloud service consists of two key elements: 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 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 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 and Security Terms)

HKMA Outsourcing SA-2

Google Cloud 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 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 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	
11.	• undertakings by the service provider that the company and its staff will abide by confidentiality rules, including taking account of the data protection principles set out in PDPO;	This is addressed in the Data Processing and Security Terms where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention. Google will ensure its employees comply with Google's security measures.	Confidentiality Data Security; Security Measures (Data Processing and Security Terms)
12.	• AIs' contractual rights to take action against the service provider in the event of a breach of confidentiality;	Refer to Row 11.	N/A
13.	• segregation or compartmentalization of AIs' customer data from those of the service provider and its other clients; and	To keep data private and secure, Google logically isolates each customer's data from that of other customers. Refer to Row 10 for more information on Google's security.	Security Measures; Data Storage, Isolation and Logging (Data Processing and Security Terms)

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
14.	• access rights to AIs' data delegated to authorized employees of the service provider on a need basis.	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. 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.	Access and Site Controls (Data Processing and Security Terms)
15.	2.5.3 AIs should notify their customers in general terms of the possibility that their data may be outsourced. They should also give specific notice to customers of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction.	This is a customer consideration.	N/A
16.	2.5.4. In the event of a termination of outsourcing agreement, for whatever reason, AIs should ensure that all customer data is either retrieved from the service provider or destroyed.	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: ● 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.	Transition Term

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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 (Data Processing and Security Terms)
17.	**2.6. Control Over Outsourced Activities**		
18.	2.6.1. In any outsourcing arrangement, AIs should ensure that they have effective procedures for monitoring the performance of, and managing the relationship with, the service provider and the risks associated with the outsourced activity.	Refer to Row 3 for more information on how you can monitor Google's performance of the Services. In addition, refer to Row 10 for more information on how you use Google's Security Products to monitor the security of your data.	N/A
19.	2.6.2. Such monitoring should cover, inter alia:		
20.	• contract performance;	Refer to Row 3 for more information on how you can monitor Google's performance of the Services (including the SLAs).	N/A
21.	• material problems encountered by 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 whitepapaer.	Significant Developments Data Incidents (Data Processing and Security Terms)
22.	• regular review of the service provider's financial condition and risk profile; and	Refer to Row 2 for information regarding Google's financial condition and risk profile.	N/A
23.	• the service provider's contingency plan, the results of testing thereof and the scope for improving it.	Refer to Row 28 for information on Google's contingency planning.	N/A
24.	2.6.3 Responsibility for monitoring the service provider and the outsourced activity should be assigned to staff with appropriate expertise.	This is a customer consideration.	N/A

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
25.	2.6.4 AIs should establish reporting procedures which can promptly escalate problems relating to the outsourced activity to the attention of the management of the AI and their service providers.	Refer to Row 3 on how you can monitor Google's performance of the Services and Row 21 on Google reporting.	N/A
26.	2.6.5 The control procedures over the outsourcing arrangement should be subject to regular reviews by the Internal Audit.	This is a customer consideration. Refer to Row 33 on the audit, access and information rights Google grants to regulated entities.	N/A
27.	**2.7. Contingency Planning**		
28.	2.7.1. Contingency plans should be maintained and regularly tested by AIs and their service providers to ensure business continuity, e.g. in the event of a breakdown in the systems of the service provider or telecommunication problems with the host country.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
29.	2.7.2. Contingency arrangements in respect of daily operational and systems problems would normally be covered in the service provider's own contingency plan. AIs should ensure that they have an adequate understanding of their service provider's contingency plan and consider the implications for their own contingency planning in the event that an outsourced service is interrupted due to failure of the service provider's system.	Refer to Row 28.	N/A
30.	2.7.3. In establishing a viable contingency plan, AIs should consider, among other things, 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.	This is a customer consideration. Refer to Row 16 for more information about how you can retrieve your data from the services. In addition, 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
31.	**2.8. Access to Outsourced Data**		
32.	2.8.1. AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA in accordance with §§55 and 56 of the Banking Ordinance and that data retrieved from the service providers are accurate and available in Hong Kong on a timely basis.	Google will enable you to access and export your data throughout the duration of our contract. Refer to Row 16 on how you can retrieve your data from the services.	Access; Rectification; Restricted Processing; Portability (Data Processing and Security Terms)

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
33.	2.8.2. Access to data by the HKMA's examiners and the AI's internal and external auditors should not be impeded by the outsourcing. AIs should ensure that the outsourcing agreement with the service provider contains a clause which allows for supervisory inspection or review of the operations and controls of the service provider as they relate to the outsourced activity.	Google grants audit, access and information rights to regulated entities, and supervisory authorities and both their appointees. Nothing in our contract is intended to limit or impede an regulated entity's or the supervisory authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help regulated entities review our Services, our contract does not contain pre-defined steps before regulated entities or supervisory authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Enabling Customer Compliance
34.	**2.9. Additional Concerns in relation to Overseas Outsourcing**		
35.	2.9.1. In addition to the issues mentioned from subsections 2.1 to 2.8 above, there are further concerns that need to be addressed in relation to overseas outsourcing:		
36.	• implications of the overseas outsourcing for AIs' risk profile - AIs should understand the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas country (e.g. legal system, regulatory regime, sophistication of technology, infrastructure);	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. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Data Processing and Security Terms) Data Security; Subprocessors (Data Processing and Security Terms) Data Location (Service Specific Terms)
37.	• right of access to customers' data by overseas authorities such as the police and tax authorities - AIs should generally obtain a legal opinion from an international or other reputable legal firm in the relevant jurisdiction on this matter. This will enable them to be	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:	Confidentiality

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	informed of the extent and the authorities to which they are legally bound to provide information. Right of access by such parties may be unavoidable due to compulsion of law. AIs should therefore conduct a risk assessment to evaluate the extent and possibility of such access taking place. AIs should notify the HKMA if overseas authorities seek access to their customers' data. If such access seems unwarranted the HKMA reserves the right to require the AI to take steps to make alternative arrangements for the outsourced activity;	• 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 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.	
38.	• notification to customers - AIs should generally notify their customers of the country in which the service provider is located (and of any subsequent changes) and the right of access, if any, available to the overseas authorities;	This is a customer consideration. Refer to Rows 36 and 37 on service location and lawful access.	N/A
39.	• right of access to customers' data for examination by the HKMA after outsourcing - AIs should not outsource to a jurisdiction which is inadequately regulated or which has secrecy laws that may hamper access to data by the HKMA or AIs' external auditors. They should ensure that the HKMA has right of access to data. Such right of access should be confirmed in writing by both AIs and their home or host authorities, as the case may be;	Refer to Row 33 on the audit, access and information rights Google grants to supervisory authorities. These rights apply regardless of the service location.	N/A
40.	• §33 of the PDPO in respect of transfer of personal data outside Hong Kong – although §33 has not yet come into operation, AIs are advised to take account of the provisions therein and the potential impact on their plans in respect of overseas outsourcing; and	This is a customer consideration. Google makes commitments to protect your data, including regarding security, use, transfer, access and retention, in the Data Processing and Security Terms.	N/A
41.	• 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

HKMA Outsourcing SA-2

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
42.	2.9.2. In case of a locally incorporated AI, a principal concern is the ability of the HKMA to exercise its legal powers under the Banking Ordinance effectively if there is limited cooperation by the service provider. Accordingly, where a local AI is planning to outsource, for example, a major part of its data processing function to outside Hong Kong, the HKMA will expect the AI to have a robust back-up system and contingency plan in an acceptable jurisdiction. The back-up system should be properly documented and regularly tested (see also subsection 2.7 above). It may be appropriate for an independent opinion on its effectiveness to be sought.	Refer to Row 33 on the audit, access and information rights Google grants to supervisory authorities. These rights apply regardless of the service location. Google will cooperate with supervisory authorities exercising their audit, information and access rights.	Enabling Customer Compliance; Regulator Information, Audit and Access