The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

This document is designed to help banks supervised by the Money Authority of Singapore (“**regulated entity**”) to consider Guidelines on Outsourcing: Banks (“**framework**”) in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: 3.3 (assessment of service providers), 3.4 (outsourcing agreement), 3.5 (use of sub-contractor(s)), 3.6 (confidentiality and security), 3.7 (business continuity management), 3.8 (monitoring and control of outsourcing arrangements), 3.9 (audit and inspection) and 3.10 (outsourcing outside of Singapore). 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.	**3.3**	**Assessment of service providers**		
2.	3.3.1	In considering, renegotiating or renewing an outsourcing arrangement, a Bank should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.	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. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud’s platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page.	N/A
3.	3.3.2	A Bank should assess all relevant aspects of the service provider, including its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the Bank to meet its obligations as a regulated entity. The due diligence should also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement. Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, should also be obtained to supplement the Bank’s assessment. Onsite visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.	Refer to Rows 4 to14.	N/A
4.	3.3.3	The due diligence should involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider’s:		
5.	(a)	experience and capability to implement and support the outsourcing arrangement over the contracted period;	Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud’s capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page.	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. You can review information about Google's historic performance of the services on our Google Cloud Service Health Dashboard.	
6.	(b) financial strength and resources (the due diligence should be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitment of major equity sponsors and ability to service commitments even under adverse conditions);	Information about Google's corporate history is available on Alphabet's Investor Relations page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A
7.	(c) corporate governance, business reputation and culture, compliance, and pending or potential litigation;	Corporate governance Refer to Row 6. Business reputation Refer to Row 5. Culture You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct, which addresses conflicts of interest Information about Google Cloud's leadership team is available on our Media Resources page. Compliance As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from	

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information. Pending litigation Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page. Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page.	
8.	(d) security and internal controls, audit coverage, reporting and monitoring environment;	Information about Google's approach to internal control environment and audit coverage is available in Google's certifications and audit reports. You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
9.	(e) risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement;	Risk management See Row 8 above. 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. Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
10.	(f) disaster recovery arrangements and disaster recovery track record;	See above.	
11.	(g) reliance on and success in dealing with sub-contractors;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors;	Google Subcontractors

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	
12.	(h) insurance coverage;	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
13.	(i) external environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates); and	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 Google Cloud services can be deployed is available on our Global Locations page. -Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: -The same robust security measures apply to all Google facilities, regardless of country / region. -Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
14.	(j) ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
15.	3.3.4 A Bank should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the Bank's hiring policies for the role they are performing, consistent with the criteria applicable to its own employees. The following are some non-exhaustive examples of what should be considered under this assessment:	Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. These checks include: -criminal checks to the extent permitted by applicable law; and	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	(a) whether they have been the subject of any proceedings of a disciplinary or criminal nature; b) whether they have been convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty); (c) whether they have accepted civil liability for fraud or misrepresentation; and (d) whether they are financially sound.	-restricted parties and global sanctions checks. Google will not permit an individual to perform the Services if a restricted parties check or global sanctions and enforcement check evidences that they are restricted under applicable law from performing the Services and the individual is not able to prove error.	
16.	Any adverse findings from this assessment should be considered in light of their relevance and impact to the outsourcing arrangement.	This is a customer consideration.	N/A
17.	3.3.5 Due diligence undertaken during the assessment process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing arrangements. A risk-based approach may be used to determine the frequency for the re-performance of due diligence for outsourcing arrangements (including intragroup arrangements). The due diligence process may vary depending on the nature, and extent of risk of the service and impact to the Bank in the event of a disruption to service or breach of security and confidentiality (e.g. reduced due diligence may be sufficient where the outsourcing arrangements are made within the Bank's group). A Bank should ensure that the information used for due diligence evaluation is sufficiently current. A Bank should also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.	This is a customer consideration.	N/A
18.	3.3.6 For the purposes of paragraph 5.2(b) of the Notices on policies on frequencies of checks, a Bank may, but is not required to, set a specific policy for each MOORS. Banks may set policies for groups or types of MOORS so long as banks ensure that the review frequency is commensurate with the risks posed by the MOORS.	This is customer consideration.	N/A
19.	**3.4 Outsourcing agreement**		
20.	3.4.1 Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements. They should also be vetted by a competent authority (e.g. the Banks' legal counsel) on their legality and enforceability.	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract	N/A
21.	3.4.2 A Bank should ensure that every outsourcing agreement addresses the risks identified at the risk evaluation and due diligence stages. Each outsourcing agreement should allow for timely renegotiation and renewal to enable the Bank to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations. It should at the very least, have provisions to address the following aspects of outsourcing:	Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.	Term and Termination

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
22.	(a) scope of the outsourcing arrangement;	The Google Cloud services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
23.	(b) performance, operational, internal control and risk management standards;	Information about Google's approach to risk management and internal control environment is available in Google's certifications and audit reports. 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.	Certification and Audit Reports
24.	(c) confidentiality and security;	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: Our infrastructure security page Our security whitepaper Our cloud-native security whitepaper Our infrastructure security design overview page Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: Security best practices Security use cases Security blueprints	
25.	(d) 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. Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor.	Business Continuity and Disaster Recovery

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	
26.	(e) monitoring and control;	Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: The Service Health Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Control You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control the Services: Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources.	Ongoing Performance Monitoring Instructions

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. Google APIs: Application programming interfaces which provide access to Google Cloud.	
27.	(f) audit and inspection	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.	Customer Information, Audit and Access Regulator Information, Audit and Access
28.	(g) notification of adverse developments	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. You can also use Personalized Service Health to receive granular alerts about Google Cloud service disruptions, as a stop in your incident response, or integrated with your incident response or monitoring tools. 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)
29.	• A Bank should specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the Bank in order for the Bank to take prompt risk mitigation measures and notify MAS of such developments under paragraph 2.2;	See above.	N/A
30.	(h) dispute resolution	Dispute resolution Refer to your Google Cloud Financial Services Contract.	Governing Law
31.	• A Bank should specify in its outsourcing agreement the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties in the agreement. The Bank should ensure that its contractual rights can be exercised in the event of a breach of the outsourcing agreement by the service provider;	Resolution Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution. Indemnification Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Support through Resolution

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Remedies If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Indemnification Services
32.	(i) default termination and early exit	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. 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.	Term and Termination Transition Term
33.	(j) applicable laws • Agreements should include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.	Refer to your Google Cloud Financial Services Contract.	Governing Law
34.	3.4.3 A Bank should have the right to terminate the outsourcing agreement in the event of default, or under any of the following circumstances:	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority	Term and Termination
	(a) by giving reasonable notice to the service provider;	See above	N/A
	(b) if the service provider or a sub-contractor, as the case may be, failed to safeguard the confidentiality or integrity of customer information of the Bank; or	See above	N/A
	(c) if there has been a demonstrable deterioration in the ability of the service provider or a sub-contractor to safeguard the confidentiality of customer information.	See above	N/A
35.	3.4.4 The minimum period to execute a termination provision should be specified in the outsourcing agreement. Other provisions should also be put in place to ensure a smooth transition when the agreement is terminated or being amended. Such provisions may facilitate transferability of the outsourced	Refer to Row 34.. 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	Transition Term

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		services to a bridge-institution or a third party. Where the outsourcing agreement involves an intra-group entity, the agreement should be legally enforceable against the intra-group entity providing the outsourced service.	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. In addition, our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance
36.	3.4.5	For the purposes of paragraph 7.1(g) in the Notices, MAS will consider directing a Bank to terminate the contract, or to stop obtaining or receiving the MOORS, when:	Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority	Term and Termination
37.	(a)	circumstances referred to in paragraph 10.3 of the Notices arise and the service provider is unwilling or unable to remediate the issues;	See above	N/A
38.	(b)	the service provider is unable or unwilling to remediate issues and the Bank did not elect to terminate the outsourcing agreement of its own accord;	See above	N/A
39.	(c)	a Bank fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the MOORS;	See above	N/A
40.	(d)	a Bank fails or is unable to implement adequate measures to address the risks arising from its ongoing outsourced relevant services in a satisfactory and timely manner;	See above	N/A
41.	(e)	adverse developments arise from the MOORS that could impact a Bank;	See above	N/A
42.	(f)	MAS or an auditor appointed by MAS, is prevented by the service provider from auditing the books, systems and premises of the service provider for any of the purposes mentioned in section 47A(10) of the Banking Act 1970 (the "Act");	See above. 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.	Regulator Information, Audit and Access
43.	(g)	where the sub-contracting agreement provides for the matter mentioned in paragraph 3.5.3(b)(iv), the Bank or any auditor appointed by the Bank, is prevented by the sub-contractor from auditing the books, systems and premises	See above. Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this,	Google Subcontractors

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		of the sub-contractor for any of the purposes mentioned in paragraph 3.5.3(b)(iv); or	Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	
44.	(h)	where the sub-contracting agreement provides for the matter mentioned in paragraph 3.5.3(b)(v), the Bank, or any person appointed by the Bank, is prevented by the sub-contractor from obtaining any record, document, report or information relating to the sub-contracting arrangement.	See above.	N/A
45.	3.4.6	MAS will endeavour to provide the Bank reasonable notice of MAS' intent to direct the Bank to terminate its outsourcing arrangement(s).	See above.	N/A
46.	3.4.7	To better protect its information, a Bank should endeavour for the requirement in paragraph 7.1(f) of the Notices on deleting, destroying or rendering unusable information upon termination to go beyond the minimally required customer information to also include non-customer information given to the service provider, except for situations where the Bank assesses that the service provider has legitimate reason(s) to retain non-customer information. The Bank should also ensure the minimum period to execute a termination provision is specified in the outsourcing agreement.	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 whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
47.	3.4.8	Each agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored. Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. These rights apply regardless of the service location.	Regulator Information, Audit and Access
48.	**3.5**	**Use of sub-contractor(s)**		

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
49.	3.5.1 A Bank should retain the ability to monitor and control the risks arising from its outsourcing arrangements when a service provider uses a sub-contractor. An outsourcing agreement should contain clauses setting out the rules and limitations on sub-contracting. A Bank should include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractor and for the sub-contractor's compliance with the provisions in its agreement with the service provider, including the prudent practices set out in these Guidelines. A Bank should ensure that the sub-contracting of any part of MOORS is subject to the Bank's prior approval.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities 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. In addition, Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights). Google will remain liable to you for any subcontracted obligations.	Google Subcontractors
50.	3.5.2 Before a Bank allows a MOORS that involves the disclosure of customer information to be subcontracted, it must obtain the written consent of the customer for the Bank to disclose the customer information to the sub-contractor. Such consent need not name the service providers to whom customer information is to be disclosed, though the scope and purpose for the disclosure should be made known.	See above	N/A
51.	3.5.3 For MOORS, a Bank should take reasonable steps, on a risk proportionate and best effort basis, to ensure that sub-contractors are held to similar standards as service providers. This could be through inclusion of appropriate provisions in its outsourcing agreement with service providers. A Bank should endeavour to ensure the following:	Google requires our subcontractors to meet the same high standards that we do. Google requires our subcontractors to comply with our contract with you and to only access and use your data to the extent required to perform the obligations subcontracted to them. Google will ensure its subcontractors comply with Google's security measures and that all persons authorized to process customer data are under an obligation of confidentiality.	Google Subcontractors Requirements for Subprocessor Engagement (Cloud Data Processing Addendum) Data Security; Access and Compliance (Cloud Data Processing Addendum)
52.	(a) where a sub-contracting arrangement involves the disclosure of customer information to a sub-contractor:	See above	N/A
53.	(i) the sub-contractor is notified in writing of the Bank's obligations of confidentiality under the Act and common law;	See above	N/A
54.	(ii) customer information is disclosed to, or accessed, collected, copied, modified, used, stored or processed by, a sub-contractor only to the extent that is necessary for the sub-contractor to perform its duties under a sub-contracting arrangement; and	See above	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
55.	(iii) the sub-contractor and its employees do not disclose any customer information of the Bank to any third party unless compelled by law, in which case the sub-contractor must notify the Bank directly or through the service provider as soon as practicable to the extent permitted by law;	See above 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 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.	Confidentiality
56.	(b) that a sub-contracting agreement includes the following provisions:		
57.	(i) the sub-contractor protects the confidentiality and integrity of all information of the Bank in its custody, in relation to the provision of the MOORS under the sub-contracting arrangement;	Refer to Row 51.	N/A
58.	(ii) the sub-contractor ensures that it and its employees only access, collect, copy, modify, use, store, or process any customer information of the Bank to the extent that is necessary for it and its employees to provide the MOORS under the sub-contracting arrangement;	Refer to Row 51.	N/A
59.	(iii) the sub-contractor ensures that it and its employees do not disclose any customer information of the Bank to any third party unless compelled by law, in which case the sub-contractor must notify the Bank directly or through the service provider as soon as practicable to the extent permitted by law;	Refer Row 51.	N/A
60.	(iv) MAS, or an auditor appointed by MAS, be allowed to audit the sub-contractor for the purposes of determining whether the sub-contractor is properly providing the MOORS under the sub-contracting arrangement and assessing:	Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
61.	(A) the ability of the sub-contractor to:	See above	N/A
62.	(AA) ensure continuity of the MOORS under the sub-contracting arrangement;	See above	N/A
63.	(BB) safeguard the confidentiality and integrity of all information in its custody, in relation to the provision of the MOORS under the sub-contracting arrangement; and	See above	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
64.	(CC)	manage its legal, reputational, technological and operational risks arising from the provision of the MOORS under the sub-contracting arrangement; and	See above	N/A
65.	(B)	the level of compliance of the sub-contractor with written laws related to the provision of the MOORS under the sub-contracting arrangement;	See above	N/A
66.	(v)	a provision that the sub-contractor, on a request by the Bank, directly or through the service provider, provides to the Bank or MAS, or any person appointed by the Bank or MAS, any record, document, report or information relating to the provision of the MOORS under the sub-contracting arrangement; and	See above	N/A
67.	(vi)	a provision that if the Bank stops obtaining or receiving the MOORS under the sub-contracting arrangement provided by the sub-contractor, the sub-contractor ensures that customer information given to the sub-contractor are deleted, destroyed or rendered unusable as soon as possible except where:	See above	N/A
68.	(A)	the sub-contractor is prohibited from doing so by written law or foreign laws, in the case where the MOORS under the sub-contracting arrangement is obtained or received overseas; or	See above	N/A
69.	(B)	in the case where the sub-contractor is a branch or office, the record, document or information is stored in a system used by the Bank which upon the termination of the sub-contracting agreement, can only be accessed by the Bank;	See above	N/A
70.	3.5.4	For the purposes of paragraph 6.3(a) of the Notices, MAS expects the notification to take place no later than 30 days. Where a notification occurs after 30 days, Banks should assess if the service provider has good reasons to do so and work with the service provider to ensure notifications are provided more promptly in the future.	This is a customer consideration.	N/A
71.	**3.6**	**Confidentiality and Security**		
72.	3.6.1	As public confidence in financial institutions is a cornerstone in the stability and reputation of the financial industry, it is vital that a Bank satisfies itself that the service provider's security policies, procedures and controls will enable the Bank to protect the confidentiality and security of customer information.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

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

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

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 Security blueprints	
73.	3.6.2 A Bank should be proactive in identifying and specifying requirements for confidentiality and security for the outsourcing arrangement. A Bank should take the following steps to protect the confidentiality and security of customer information:	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures; (Cloud Data Processing Addendum)
74.	(a) State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which each party has the right to change security requirements. The outsourcing agreement should also address:	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers. Google continues to improve the security of 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, these updates apply to all customers at the same time. Google will not update	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		our security measures in a way that results in a material reduction of the security of the services.	
75.	(i) the issue of the party liable for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the Bank; and	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. To assist customers with their own incident response, Google's notification will describe: -the nature of the Data Incident including the Customer resources impacted; -the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; -the measures, if any, Google recommends that Customer take to address the Data Incident; and -details of a contact point where more information can be obtained. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Autonomic Security Operations (ASO) solution: -delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. -enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. Here are some examples: -Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. -Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud environment. -Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud resources and changes to resources including VM instances, images, and operating systems.	Data Incidents (Cloud Data Processing Addendum)
76.	(ii) the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service;	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Protection of Customer Data
77.	(b) Disclose customer information to the service provider only on a need-to-know basis;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			you provide to the services under your account and may access your data on the services at any time.	
78.	(c)	Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets, particularly where multi-tenancy arrangements are present at the service provider; and	Refer to Row 72. To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
79.	(d)	Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the Bank breaches of confidentiality in relation to customer information.	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 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. Google 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.	Certifications and Audit Reports Customer Information, Audit and Access Data Incidents (Cloud Data Processing Addendum)
80.	**3.7**	**Business Continuity Management**		
81.	3.7.1	A Bank should ensure that its business continuity is not compromised by outsourcing arrangements, in particular, the operation of its critical business services and functions as stipulated under the MAS Business Continuity Management (BCM) Guidelines and critical systems as stipulated under the MAS Notice on Technology Risk Management. A Bank should adopt the sound practices and standards contained in the BCM Guidelines, in evaluating the impact of outsourcing on its risk profile and for effective BCM.	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications.	
82.	3.7.2 In line with the BCM Guidelines, a Bank should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangements can be adequately mitigated such that the Bank remains able to meet its business obligations in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider. These should include taking the following steps:		
83.	(a) Incorporate the necessary contractual requirements and verify that the service provider has in place satisfactory business continuity plans (BCP) that are commensurate with the nature, scope and complexity of the outsourcing arrangement;	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. Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
84.	(b) Proactively seek assurance on the state of BCP preparedness of the service provider. It should ensure the service provider regularly tests its BCP to ascertain that the recovery objectives can be met. The Bank should require the service provider to notify it of any test finding that may affect the service provider's performance. The Bank should also require the service provider to notify it of any substantial changes in the service provider's BCP and of any adverse development that could substantially impact the service provided to the Bank; and	Google recognizes that regulated entities are expected to set impact tolerances on the assumption that a disruption will occur. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud. 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	Business Continuity and Disaster Recovery Significant Developments

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		is available at our Incidents & the Google Cloud dashboard page. You can also use Personalized Service Health to receive granular alerts about Google Cloud service disruptions, as a stop in your incident response, or integrated with your incident response or monitoring tools.	
85.	(c) Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the Bank will be able to continue business operations and that all documents, records of transactions and information previously given to the service provider should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.	Exit planning Google recognizes that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: -Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. -Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. -Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards. Deletion 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 whitepaper.	Data Export (Cloud Data Processing Addendum) Deletion on Termination (Cloud Data Processing Addendum)
86.	3.7.3 A Bank should involve its service providers, where applicable, in the validation and testing of its BCPs to ensure that BCP testing is complete and meaningful, and to gain assurance on the functionality and effectiveness of its BCPs. Similarly, a Bank could take part in its service providers' business continuity and disaster recovery tests. Such tests would also serve to familiarise the Bank and	Refer to Rows 83 and 84. In addition to testing our own environments, Google also provides a number of tools and resources that enable regulated entities to independently test their Google Cloud deployments.	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		the service provider with the recovery processes, as well as improve the coordination between the parties involved.	Our Disaster Recovery Scenarios for Data and Disaster Recovery for Applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively. You can also implement the following to help with your own testing: **Automate infrastructure provisioning with Deployment Manager**. You can use Deployment Manager to automate the provisioning of VM instances and other Google Cloud infrastructure. If you're running your production environment on premises, make sure that you have a monitoring process that can start the disaster recovery process when it detects a failure and can trigger the appropriate recovery actions. **Monitor and debug your tests with Cloud Logging and Cloud Monitoring.** Google Cloud has excellent logging and monitoring tools that you can access through API calls, allowing you to automate the deployment of recovery scenarios by reacting to metrics. When you're designing tests, make sure that you have appropriate monitoring and alerting in place that can trigger appropriate recovery actions.	
87.	3.7.4	A Bank should consider worst case scenarios in developing its BCPs for its outsourcing arrangements. Some examples of these scenarios are unavailability of service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions that result in collateral impact on both the Bank and the service provider. Where the interdependency on a Bank in the financial system is high, the Bank should maintain a higher state of business continuity preparedness. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate interdependency risk.	Refer to Row 84.	N/A
88.	**3.8**	**Monitoring and control of outsourcing arrangements**		
89.	3.8.1	A Bank should establish a structure for the management and control of its outsourcing arrangements. Such a structure will vary depending on the nature and extent of risks in the outsourcing arrangements. As relationships and interdependencies in respect of outsourcing arrangements increase in materiality and complexity, a more rigorous risk management approach should be adopted. A Bank also has to be more proactive in its relationship with the service provider (e.g. having frequent meetings) to ensure that performance, operational, internal control and risk management standards are upheld. A Bank should ensure that outsourcing agreements with service providers contain clauses to address the Bank's monitoring and control of outsourcing arrangements.	Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: The Service Health Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response,	Ongoing Performance Monitoring

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Control Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the following functionality of the Services: Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. Google APIs: Application programming interfaces which provide access to Google Cloud. Google will comply with the regulated entity's instructions.	Instructions
90.	3.8.2	A Bank should put in place all the following measures for effective monitoring and control of any MOORS:		
91.	(a)	Maintain a register of outsourcing arrangements and ensure that the register is readily accessible for review by the board and senior management of the Bank. The register should be updated promptly and form part of the oversight and governance reviews undertaken by the board and senior management of the Bank, similar to those described in paragraph 3.1;	Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
92.	(b) Establish multi-disciplinary outsourcing management groups with members from different risk and internal control functions including legal, compliance and finance, to ensure that all relevant technical issues and legal and regulatory requirements are met. The Bank should allocate sufficient resources, in terms of both time and skilled manpower, to the management groups to enable its staff to adequately plan and oversee the entire outsourcing lifecycle;	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
93.	(c) Establish outsourcing management control groups to monitor and control the outsourced relevant service on an ongoing basis. There should be policies and procedures to monitor service delivery and the confidentiality and security of customer information, for the purpose of gauging ongoing compliance with agreed service levels and the viability of the Bank's operations. Such monitoring should be regular and validated through the review of reports by auditors of the service provider or audits commissioned by the Bank	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 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
94.	(d) Reporting policies and procedures	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. 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)
95.	Reports on the monitoring and control activities of the Bank should be reviewed by its senior management and provided to the board for information. The Bank should ensure that monitoring metrics and performance data are not aggregated with those belonging to other customers of the service provider. The Bank should also ensure that any adverse development arising in any outsourcing arrangement is brought to the attention of the senior management of the Bank and service provider, or to the Bank's board, where warranted, on a	Refer to Rows 89 to 94.	N/A

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		timely basis. When an adverse development occurs, prompt actions should be taken by a Bank to review the outsourcing relationship for modification or termination of the agreement; and		
96.	(e)	Perform comprehensive pre- and post- implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements. If an outsourcing arrangement is materially amended, a comprehensive due diligence of the outsourcing arrangement should also be conducted.	This is a customer consideration.	N/A
97.	**3.9**	**Audit and inspection**		
98.	3.9.1	A Bank's outsourcing arrangements should not interfere with the ability of the Bank to effectively manage its business activities or impede MAS in carrying out its supervisory functions.	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
99.	3.9.2	A Bank should include, in all its outsourcing agreements for MOORS, clauses that allow the Bank to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the Bank. The Bank should also obtain copies of any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's or its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractor, in relation to the outsourcing arrangement.	Audit rights 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 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 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Customer Information, Audit and Access Certifications and Audit Reports
100.	3.9.3	A Bank should endeavour to subject any sub-contractor, that a service provider (including any disaster recovery and backup service providers) may engage in the Bank's MOORS, to the audit requirements and expectations applied to the	Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google	Google Subcontractors

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		service provider. MAS will endeavour to provide the Bank reasonable notice of MAS' intent to exercise its inspection rights and share its findings with the Bank where appropriate.	will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	
101.	3.9.4	A Bank should ensure that independent audits and/or expert assessments of its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the Bank should consider the nature and extent of risk and impact to the Bank from the outsourcing arrangements. The scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security and control environment, incident management process (for material breaches, service disruptions or other material issues) and the Bank's observance of the expectations in these Guidelines in relation to the outsourcing arrangement.	Audit rights 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. Audit reports Google is audited at least once a year for each audited framework. You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Customer Information, Audit and Access Certifications and Audit Reports
102.	3.9.5	The independent audit and/or expert assessment on the service provider and its sub-contractors may be performed by the Bank's internal or external auditors, the service provider's external auditors or by agents appointed by the Bank (e.g. audits commissioned by multiple Banks using the same service provider). The appointed persons should possess the requisite knowledge and skills to perform the audit, and be independent of the unit or function performing the outsourcing arrangement. Senior management should ensure that appropriate and timely remedial actions are taken to address the audit findings. Banks and service providers should have adequate processes in place to ensure that remedial actions are satisfactorily completed. Actions taken by the service provider to address the audit findings should be appropriately validated by the Bank before closure. Where necessary, the relevant persons who possess the requisite knowledge and skills should be involved to validate the effectiveness of the security and control measures taken.	Auditing party Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party. Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world. Remediation 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.	Certifications and Audit Reports Customer Information, Audit and Access
103.	3.9.6	Significant issues and concerns should be brought to the attention of the senior management of the Bank and service provider, or to the Bank's board, where warranted, on a timely basis. Actions should be taken by the Bank to review the outsourcing arrangement if the risk posed is no longer within the Bank's risk tolerance.	This is a customer consideration.	N/A
104.	3.9.7	Copies of audit reports should be submitted by the Bank to MAS upon request. A Bank should also, upon request, provide MAS with other reports or information on the Bank and service provider that is related to the outsourcing arrangement.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access.	Regulator Information, Audit and Access

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
105.	3.9.8 Audits and/or expert assessments performed as part of a certification process (but not self-attestations) may be relied on to meet requirements or expectations on audit provided that such audit or assessments are performed by independent and competent auditors. A Bank must also satisfy itself that the audit's scope and methodology allow the Bank to determine the ability of the service provider to perform the outsourcing arrangement (e.g. design, implementation and effectiveness of controls) and the adequacy of the service provider's risk management framework and capabilities. Audit reports must fulfil requirements set out in the Notices. Banks may also rely on pooled audits or third-party certification (of their service providers) performed by independent parties.	You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope. Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.	Certifications and Audit Reports
106.	**3.10 Outsourcing outside Singapore**		
107.	3.10.1 The engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in a foreign country may expose 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. In its risk management of such outsourcing arrangements, a Bank should take into account, as part of its due diligence, and on a continuous basis: (a) government policies; (b) political, social, economic conditions; (c) legal and regulatory developments in the foreign country; and (d) the Bank's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.	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. 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 Google Cloud services can be deployed is available on our Global Locations page. -Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: -The same robust security measures apply to all Google facilities, regardless of country / region. -Google makes the same commitments about all its subprocessors, regardless of country / region.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

The Monetary Authority of Singapore - Guidelines on Outsourcing (Banks)

Google Cloud 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 Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored. Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. These rights apply regardless of the service location.	Data Location (Service Specific Terms) Regulator Information, Audit and Access Customer Information, Audit and Access
108.	A Bank should also be aware of the disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. As information and data could be moved to primary or backup sites located in foreign countries, the risks associated with the medium of transport, be it physical or electronic, should also be considered.	See above	N/A
109.	3.10.2 MOORS with service providers located outside Singapore should be conducted in a manner so as not to hinder MAS' efforts to supervise the Singapore business activities of the Bank (i.e. from its books, accounts and documents) in a timely manner, in particular:	See above.	N/A
110.	(a) A Bank should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements.	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
111.	(b) A Bank should not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by MAS or agents appointed by MAS to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions. A Bank must at least commit to retrieve information readily from the service provider should MAS request for such information.	Refer to Row 110.	N/A