Last updated October 2019

Engagement with MAS on Outsourcing

4.1 - Observance of the MAS Guidelines

Item #	MAS Guideline Recommended Practices	Google Cloud Support
4.1.3	MAS may require an institution to modify, make alternative arrangements or reintegrate an outsourced service into the institution where one of the following circumstances arises:	--
4.1.3(a)	An institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the outsourcing arrangement	Primarily customer responsibility to satisfy this requirement. Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO 27001 certification. Google makes available its SOC2/SOC3 reports and ISO 27001, 27017, and 27018 certifications and similar third-party audit or certification reports available to customers. For a full list of available certifications and compliance materials, please refer to https://cloud.google.com/security/compliance.
4.1.3(b)	An institution fails or is unable to implement adequate measures to address the risks arising from its outsourcing arrangements in a satisfactory and timely manner	Primarily customer responsibility to satisfy this requirement. Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO 27001 certification.
4.1.3.(c)	Adverse developments arise from the outsourcing arrangement that could impact an institution	Primarily customer responsibility to satisfy this requirement. Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. If Google becomes aware of a data incident, Google will notify the Customer promptly and without undue delay and promptly take reasonable steps to minimize harm and secure Customer Data.
4.1.3.(d)	MAS' supervisory powers over the institution and ability to carry out MAS' supervisory functions in respect of the institution's services are hindered	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite as well as in the Financial Services Agreement or Addendum (as applicable) signed between Google and the Customer.
4.1.3.(e)	The security and confidentiality of the institution's customer information is lowered due to changes in the control environment of the service provider.	Primarily customer responsibility to satisfy this requirement. Google enables customers to bring their own change and configuration management tools to Google Cloud. The customer is responsible for their own change management processes, including defining appropriate roles and responsibilities.

4.2 - Notifications of Adverse Developments

Item #	MAS Guideline Recommended Practices	Google Cloud Support

4.2.1	An institution should notify MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the institution. Such adverse developments include any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the institution's customer information.	Primarily customer responsibility to satisfy this requirement. Google supports Customers in identifying developments regarding the services. In particular: (a) Services Levels - Google provides the services in accordance with public SLAs. The SLAs are available at https://cloud.google.com/terms/sla/. (b) Service Status Dashboard - The Google Cloud Status Dashboard provides information about the current and past status of the services at https://status.cloud/google.com/. Customers can use the Status Dashboard to monitor the availability and health of the services on a daily basis. Status can include service disruptions, outages or information messages about a temporary issue. (c) Monitoring tools - Google provides tools that customers can use to monitor their own use of the service to ensure compliance with their own internal policies/procedures. These tools also make it easy for customers to create custom dashboards and set alerts when issues occur. For example: Google Cloud Logging and Google Cloud Monitoring, which allow customers to collect and analyse request logs and monitor the availability of their infrastructure services. (d) Incident Response Process - Google has a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data. More information can be found at: https://cloud.google.com/security/incident-response/
5.3 - Evaluation of Risks		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.1	Intentionally omitted	Intentionally omitted
5.2	Intentionally omitted	Intentionally omitted
5.3.1	The FI should establish a framework for risk evaluation to ensure that an outsourcing arrangement does not result in the risk management, internal control, business conduct or reputation of its operation being compromised or weakened.	Primarily customer responsibility to satisfy this requirement. Customers can use tools available as part of Google's standard offering to help them perform the required risk evaluation. In particular, Google provides customers with: 1. controls, which customers can use to configure the services to meet their specific requirements; and 2. information about Google's security practices, so customers can assess if they are appropriate given how they wish to use the services. Google provides comprehensive external documentation and white papers detailing our security infrastructure and operational model. Google also maintains an internal ISMS as a risk management framework and evidence of its effectiveness is provided via our ISO 27001 certification. In addition, Google makes available its SOC2/SOC3 reports and ISO 27001, 27017, and 27018 certifications and similar third-party audit or certification reports available to customers. For a full list of available certifications and compliance materials, please refer to https://cloud.google.com/security/compliance.
5.3.2	Intentionally omitted	Intentionally omitted
5.4 - Assessment of Service Providers		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.4.1	In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.	Primarily customer responsibility to satisfy this requirement. Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs. We have dedicated teams of engineers and compliance experts who support our customers in meeting their current and emerging regulatory compliance and risk management obligations. Our approach includes collaborating with customers to understand and address their specific regulatory obligations. Together with our reports and certifications, we assist our customer in documenting an integrated controls and governance framework.

5.4.2	An institution 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 institution 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 institution's assessment. Onsite visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.	Primarily customer responsibility to satisfy this requirement. Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security. More information on Google's contractual commitments can be found under Section 7.4 and 7.5 of the Data Processing and Security Terms (DPST) for GCP and Section 7.4 and 7.5 of the Data Processing Amendment (DPA) for G Suite. In addition, pursuant to the Financial Services Agreement or Addendum (as applicable), Google will allow the institution and/or its auditor to review information about the services operations and controls and discuss it without Google subject matter experts; audit and inspect the services used by the institution and access Google's premises used to provide those services to do so. Please also see our responses to Items 5.4.3(a) to 5.4.3(j). More information on Google's physical and IT security controls can be found here: - Google Cloud Platform Data Processing and Security Terms, Appendix 2: Security Measures (https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures) - G Suite Data Processing Amendment, Appendix 2: Security Measures (https://gsuite.google.com/terms/dpa_terms.html?_ga=2.115519814.-1599980538.1564069885) - Google Infrastructure Security Design Overview (https://cloud.google.com/security/infrastructure/design/) - Google Cloud Security Whitepaper (https://cloud.google.com/security/overview/whitepaper) - Google Cloud Security and Compliance Whitepaper (https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf).
5.4.3	The due diligence should involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider's:	--
5.4.3(a)	experience and capability to implement and support the outsourcing arrangement over the contracted period	Primarily customer responsibility to satisfy this requirement. Google's world-class security, experience in hybrid and multi-cloud strategies, and innovations in machine learning and artificial intelligence have made it a leader in cloud services. Please see below links for more information on how Google has built a global scale technical infrastructure designed to provide security through the entire information processing lifecycle at Google: - Google's Infrastructure Security Design Overview (https://cloud.google.com/security/infrastructure/design/) - Google Cloud's Security Whitepaper (https://cloud.google.com/security/overview/whitepaper)
5.4.3(b)	financial strength and resources	Primarily customer responsibility to satisfy this requirement. Information on Alphabet's financial numbers by quarter can be found here: https://abc.xyz/investor/
5.4.3(c)	corporate governance, business reputation and culture, compliance, and pending or potential litigation	Primarily customer responsibility to satisfy this requirement. Relevant information is available in: - Alphabet, Inc's annual reports at https://abc.xyz/investor/.; - Alphabet, Inc.'s Code of Conduct at https://abc.xyz/investor/other/code-of-conduct.html; and, - Google's Code of Conduct at https://abc.xyz/investor/other/google-code-of-conduct.html
5.4.3(d)	security and internal controls, audit coverage, reporting and monitoring environment	Primarily customer responsibility to satisfy this requirement. Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security. Google has mapped its security controls to the requirements of the AICPA Trust Services Critieria (SOC2), NIST 800-53, and ISO 27002. Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. Google also provide audit assertions using industry accepted formats. For more details, please refer to: https://cloud.google.com/security/compliance.

5.4.3(e)	risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement	Primarily customer responsibility to satisfy this requirement. Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security. Google has mapped its security controls to the requirements of the AICPA Trust Services Critieria (SOC2), NIST 800-53, and ISO 27002. Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. Google also provide audit assertions using industry accepted formats. For more details, please refer to: https://cloud.google.com/security/compliance.
5.4.3(f)	disaster recovery arrangements and disaster recovery track record	Primarily customer responsibility to satisfy this requirement. Google will maintain policies, procedures, and arrangements to minimize disruptions to the Services caused by disasters or other events that disrupt the operations and resources required to provide the Services (the “BCDR Plan”). Customer may review a summary of (a) the then-current BCDR Plan, and (b) the results of the most recent BCDR Plan tests. Google will test and review the BCDR Plan at least annually. Google will remediate issues identified during testing and if needed update the BCDR Plan. Google will not degrade the BCDR Plan and ensure that it remains current with industry standards.
5.4.3(g)	reliance on and success in dealing with sub-contractors	Primarily customer responsibility to satisfy this requirement. Google maintains a robust vendor management program. Vendors who work with Google are required to comply with all relevant information security and privacy policies. Under the Financial Services Agreement or Addendum (as applicable), if Google subcontracts any of its obligations, Google will retain responsibility for, and oversight of, all subcontracted obligations; and ensure that Google subcontractors comply with the contract. To enable the institution to retain oversight of any subcontracting, Google will provide the institution with information about Google's subcontractors, notify the institution of changes to Google's subcontractors; and give the institution the opportunity to terminate the contract if they have concerns about a new subcontractor.
5.4.3(h)	insurance coverage	The Financial Services Agreement or Addendum (as applicable) sets out the insurance coverage that Google will maintain during the term of its contract with the institution. Upon request by the institution, Google will provide the institution with certificates of insurance evidencing the insurance coverage required under the Financial Services Agreement or Addendum (as applicable).
5.4.3(i)	external environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates)	Primarily customer responsibility to satisfy this requirement. Google continuously monitors the compliance landscape and make adjustments to our policies and practices as needed. Ultimately, it is the customer's responsibility to configure its services and to be in compliance with any requirements relevant to its operations or jurisdictions.
5.4.3(j)	ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.	Primarily customer responsibility to satisfy this requirement. We continuously monitor the compliance landscape and make adjustments to our policies and practices as needed. Ultimately, it is the customer’s responsibility to configure its services and to be in compliance with any requirements relevant to its operations or jurisdictions. In addition, Google recognizes that the institution may require assistance from Google to enable them to monitor the services to ensure compliance with applicable laws and regulations. Google commits under the Financial Services Agreement or Addendum (as applicable) to work with the institution to provide the assistance as set out in the Financial Services Agreement or Addendum (as applicable).
5.4.4	The institution should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the institution’s hiring policies for the role they are performing, consistent with the criteria applicable to its own employees.	Primarily customer responsibility to satisfy this requirement. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional role-specific privacy and security training may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design, and automated vulnerability testing tools. Privacy and security training are required annually. All Google employees also undergo background checks where local labor law or statutory regulations permit. Google may conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position. For further information on employee onboarding and security and privacy training, please refer to our Security White Paper (https://cloud.google.com/security/overview/whitepaper)

5.4.5	Intentionally omitted	Intentionally omitted
5.5 - Outsourcing Agreement		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.5.1	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.	The agreement between Google and the institution sets out the scope of the arrangement and the respective commitments of the parties. Generally, financial customers can contract with Google for services as follows: - via a Cloud Master Agreement ("CMA General Terms") incorporating the relevant Services Schedule, the Financial Services Addendum ("Financial Services Addendum" or "Addendum") and the Order Form; or - via a Financial Services Cloud Master Agreement ("Financial Services Agreement")(available late Q4 2019) incorporating the relevant Services Schedule and the Order Form. The CMA General Terms or the Financial Services Agreement set out terms that describe the business and legal relationship between customer and Google relating to customer's use of Google Cloud services. The respective Services Schedule sets out terms that describe the services that Google will provide to the customer. The corresponding Order Form is the operative document that, once signed, directs Google to make services available to the customer. Once the parties complete and execute an Order Form, Google will provide the services to the customer in accordance with the applicable Service Level Agreements (SLAs), which are publically available at https://gsuite.google.com/terms/sla.html. In addition, the Data Processing and Security Terms or DPST (for GCP Services) and Data Processing Amendment to G Suite or DPA (for GSuite services) reflect the parties' agreement with respect to the terms governing the processing and security of Customer Data under the Agreement. The DPST is available at: https://cloud.google.com/terms/data-processing-terms and the DPA is available at: https://gsuite.google.com/terms/dpa_terms.html The Financial Services Agreement and Financial Services Addendum provide contractual provisions that regulated financial services customers may require for regulatory compliance, in addition to the standard Google cloud services offering (i.e. the features and functionality of the Google cloud services and the contract).
5.5.2	An institution 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 institution 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:	--
5.5.2(a)	Scope of the outsourcing arrangement	Primarily customer responsibility to satisfy this requirement. Please see our response to Item 5.5.1 above. In addition, the complete list of services that form Google Cloud Platform is available at the Google Cloud Platform Services Summary: https://cloud.google.com/terms/services. The services summary for GSuite is available at: https://gsuite.google.com/terms/user_features.html Although Google makes resources and tools available, it is the customer who chooses which to use, how to use them and for what purpose. The customer can choose to change how it uses the service at any time. As such the customer determines the scope of the outsourcing arrangement.
5.5.2(b)	Performance, operational, internal control and risk management standards	Primarily customer responsibility to satisfy this requirement. These requirements are covered in the Data Processing Amendment or DPA (for GSuite), the Data Processing and Security Terms or DPST (for GCP) and the Service Level Agreement (SLA). The DPA and DPST contain the privacy and security practices, and internal controls that Google implements. The SLA sets out Google's service level commitments.
5.5.2(c)	Confidentiality and security	Primarily customer responsibility to satisfy this requirement. The General Terms or the FSCMA set out Google's commitments as to confidentiality under "Confidentiality". The DPST (for GCP) and the DPA (for GSuite) set out Google's commitments as to security.
5.5.2(d)	Business continuity management	Primarily customer responsibility to satisfy this requirement. Google's commitments to business continuity management are set out in the Financial Services Agreement or Addendum (as applicable) under "Business Continuity and Disaster Recovery". Please also see our responses to Item 5.4.3(e).

5.5.2(e)	Monitoring and control	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding monitoring and control can be found under Appendix 2: Security Measures of the Data Processing and Security Terms (DPST) for GCP and Appendix 2: Security Measures of the Data Processing Amendment (DPA) for G Suite. - Google Cloud Platform Data Processing and Security Terms, Appendix 2: Security Measures (https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures) - G Suite Data Processing Amendment, Appendix 2: Security Measures (https://gsuite.google.com/terms/dpa_terms.html?_ga=2.115519814.-1599980538.1564069885)
5.5.2(f)	Audit and inspection	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP, Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and the Financial Services Agreement or Addendum (as applicable).
5.5.2(g)	Notification of adverse developments	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments in this regard are set out at Section 7.2.1 of the Data Processing and Security Terms (DPST) for GCP and Section 7.2.1 of the Data Processing Amendment (DPA) for G Suite. Please also see our response to Item 4.2.1
5.5.2(h)	Dispute resolution	Primarily customer responsibility to satisfy this requirement. If the institution and Google have a dispute, the dispute resolution provisions would be described in the agreement between Google and the institution. This is set out under "Governing Law" in the "Miscellaneous" section of the CMA General Terms or the Financial Services Agreement (as applicable). Please also see our response to Item 5.5.2(i).
5.5.2(i)	Default termination and early exit	Primarily customer responsibility to satisfy this requirement. Institution has express termination rights for material breach under the contract. Please see the "Term and Termination" section of the CMA General Term or the Financial Services Agreement (as applicable). Institution also has the right to terminate for convenience, including termination as required by the Regulator. The Financial Services Agreement or Addendum (as applicable) also provides for business continuity upon exit, in that institution can request for a transition term for the continued provision of services, and transition assistance to migrate workloads and applications or otherwise transition the institution's use of the services.
5.5.2(j)	Sub-contracting	Primarily customer responsibility to satisfy this requirement. Under the Financial Services Agreement or Addendum (as applicable), if Google subcontracts any of its obligations, Google will retain responsibility for, and oversight of, all subcontracted obligations; and ensure that Google subcontractors comply with the contract. To enable the institution to retain oversight of any subcontracting, Google will provide the institution with information about Google's subcontractors, notify the institution of changes to Google's subcontractors; and give the institution the opportunity to terminate the GCP contract if they have concerns about a new subcontractor, all pursuant to the Financial Services Agreement or Addendum (as applicable).
5.5.2(k)	Applicable Laws	Primarily customer responsibility to satisfy this requirement. The applicable law provision is set out under "Governing Law" in the "Miscellaneous" section of the CMA General Terms or the Financial Services Agreement (as applicable).
5.5.3	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.	Primarily customer responsibility to satisfy this requirement. The agreement with an institution with a billing address in Singapore will be entered into by Google Asia Pacific Pte Ltd, a company incorporated in Singapore.
5.6 - Confidentiality and Security		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**

5.6.1	As public confidence in institutions is a cornerstone in the stability and reputation of the financial industry, it is vital that an institution satisfies itself that the service provider's security policies, procedures and controls will enable the institution to protect the confidentiality and security of customer information.	Primarily customer responsibility to satisfy this requirement. Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security. More information on Google's contractual commitments can be found under Section 7.4 and 7.5 of the Data Processing and Security Terms (DPST) for GCP and Section 7.4 and 7.5 of the Data Processing Amendment (DPA) for G Suite. More information on Google's physical and IT security controls can be found here: - Google Cloud Platform Data Processing and Security Terms, Appendix 2: Security Measures (https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures) - G Suite Data Processing Amendment, Appendix 2: Security Measures (https://gsuite.google.com/terms/dpa_terms.html?_ga=2.115519814.-1599980538.1564069885) - Google Infrastructure Security Design Overview (https://cloud.google.com/security/infrastructure/design/) - Google Cloud Security Whitepaper (https://cloud.google.com/security/overview/whitepaper) - Google Cloud Security and Compliance Whitepaper (https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf)
5.6.2	An institution should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution should take the following steps to protect the confidentiality and security of customer information:	--
5.6.2(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:	Primarily customer responsibility to satisfy this requirement. The security of a cloud service consists of 2 key elements: (a) security of the underlying infrastructure and (b) security of data and applications in the cloud. Google is responsible for the security of the underlying infrastructure (hardware, software, networking and facilities) that supports cloud services. Although Google cannot customize security controls for individual customers, we provide detailed information about our security practices and the standards they meet so that customers can understand them. Google's security commitments are provided in the Data Processing and Security Terms (for GCP) and the Data Processing Amendment (for GSuite). Customer is responsible for implementing and operating security measures used to determine and ensure the security of their data and applications in the cloud.
5.6.2(a)(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 institution	Primarily customer responsibility to satisfy this requirement. Please refer to the section on "Liability" in the General Terms or the FSCMA. In addition, Google can agree to reimburse Customer for certain remediation costs directly resulting from certain security obligation breaches.
5.6.2(a)(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	Primarily customer responsibility to satisfy this requirement. Googl Cloud's data processing amendments describe our commitment to protecting customer data. They state that Google will not process data for any other purpose other than to fulfill our contractual obligations. Section 5.2 of the Data Processing and Security Terms for Google Cloud Platform and Section 5.2 of the Data Processing Amendment for G Suite outline those commitments. In addition, under the "Confidentiality" section of the General Terms and FSA, Google commits to only use the customer's confidential information (which includes content provided through the services) to fullfill its obligations under the Agreement. Google will not disclose customer's confidential information to third parties other than delegates who need to know and have a legal obligation to keep it confidential. Google will ensure that its delegates are also subject to the same non-disclosure and use obligations.
5.6.2(b)	Disclose customer information to the service provider only on a need-to-know basis	Primarily customer responsibility to satisfy this requirement.
5.6.2(c)	Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets, particularly where multitenancy arrangements are present at the service provider	Primarily customer responsibility to satisfy this requirement. 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 personal data. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users. See https://cloud.google.com/security/overview/whitepaper. The above is also set out at Appendix 2: Security Measures of the DPST (for GCP) and DPA (for GSuite).

5.6.2(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 institution breaches of confidentiality in relation to customer information.	Primarily customer responsibility to satisfy this requirement. Google makes available its SOC2/SOC3 reports and ISO 27001, 27017, and 27018 certifications and similar third-party audit or certification reports available to customers. For a full list of available certifications and compliance materials, please refer to https://cloud.google.com/security/compliance. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP, Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Addendum and the FSCMA (as applicable).
5.7 - Business Continuity Management		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.7.1	An institution should ensure that its business continuity is not compromised by outsourcing arrangements, in particular, of the operation of its critical systems as stipulated under the Technology Risk Management Notice. An institution should adopt the sound practices and standards contained in the Business Continuity Management ("BCM") Guidelines issued by MAS, in evaluating the impact of outsourcing on its risk profile and for effective BCM.	Primarily customer responsibility to satisfy this requirement. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs. In addition, Google Cloud maintains a Business Continuity and Disaster Recovery Plan that addresses BC/DR planning for all GCP Services. The program in place aligns to Alphabet Inc.'s broader business continuity plans.
5.7.2	In line with the BCM Guidelines, an institution should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that the institution remains able to conduct its business with integrity and competence 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:	--
5.7.2(a)	Determine 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. Outsourcing agreements should contain BCP requirements on the service provider, in particular, recovery time objectives ("RTO"), recovery point objectives ("RPO"), and resumption operating capacities	Primarily customer responsibility to satisfy this requirement. Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google's highly redundant infrastructure also helps protect our customers from data loss. Essential hardware in Google data centers are hot swappable. Google maintains a dashboard for service availability information and service issues: - https://status.cloud.google.com/ - https://www.google.com/appsstatus
5.7.2(b)	Proactively seek assurance on the state of BCP preparedness of the service provider, or participate in joint testing, where possible. It should ensure the service provider regularly tests its BCP plans and that the tests validate the feasibility of the RTO, RPO and resumption operating capacities. Such tests would serve to familiarise the institution and the service provider with the recovery processes as well as improve the coordination between the parties involved. The institution should require the service provider to notify it of any test finding that may affect the service provider's performance. The institution should also require the service provider to notify it of any substantial changes in the service provider's BCP plans and of any adverse development that could substantially impact the service provided to the institution	Primarily customer responsibility to satisfy this requirement. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs. In addition, Google Cloud maintains a Business Continuity and Disaster Recovery Plan that addresses BC/DR planning for all GCP Services. The program in place aligns to Alphabet Inc.'s broader BCMP. Essential hardware in Google data centers are hot swappable. Google maintains a dashboard for service availability information and service issues: - https://status.cloud.google.com/ - https://www.google.com/appsstatus
5.7.2(c)	Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the institution 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	Primarily customer responsibility to satisfy this requirement. Google will enable customers to access, rectify, delete and export their data. See Section 9.1 (Access; Rectification; Restricting Processing; Portability) of the DPA and DPST. In addition, on termination of the contractual relationship, Google will comply with the customer's instruction to delete all Customer Data from Google's systems. See Section 6 (Data Deletion) of the DPA and DPST.
5.7.3	For assurance on the functionality and effectiveness of its BCP plan, an institution should design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement. For tests to be complete and meaningful, the institution should involve the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff. Similarly, the institution should take part in its service providers' BCP and disaster recovery exercises.	Primarily customer responsibility to satisfy this requirement. Google maintains and regularly tests business continuity planning and disaster recovery programs that are intended to minimize disruptions to the services. Customer can monitor Google's performance of the services on an ongoing basis using the functionality of the services. Institutions can and should implement their own disaster recovery and business continuity programs. The Google program can support a customer's own program, but it cannot substitute it.

5.7.4	The institution should consider worst case scenarios in its business continuity plans. 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 institution and the service provider. Where the interdependency on an institution in the financial system is high, the institution 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	Primarily customer responsibility to satisfy this requirement. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs. In addition, Google Cloud maintains a Business Continuity and Disaster Recovery Plan that addresses BC/DR planning for all GCP Services. The program in place aligns to Alphabet Inc.'s broader business continuity plans.
5.8 - Monitoring and Control of Outsourcing Arrangements - This section is intentionlly omitted		
5.9 - Audit and Inspection		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.9.1	An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives.	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP, Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite and under the Financial Services Agreement or Addendum (as applicable).
5.9.2	An institution should include, in all its outsourcing agreements for material outsourcing arrangements, clauses that:	--
5.9.2(a)	allow the institution to conduct audits on the service provider and its subcontractors, whether by its internal or external auditors, or by agents appointed by the institution; and to 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	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Agreement or Addendum (as applicable).
5.9.2(b)(i) & 5.9.2(b)(ii)	allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution to: i) access and inspect the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors; and ii) access any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement.	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP, Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite and under the Financial Services Agreement or Addendum (as applicable).
5.9.3	Outsourcing agreements for material outsourcing arrangements should also include clauses that require the service provider to comply, as soon as possible, with any request from MAS or the institution, to the service provider or its sub-contractors, to submit any reports on the security and control environment of the service provider and its sub-contractors to MAS, in relation to the outsourcing arrangement	Primarily customer responsibility to satisfy this requirement. Under the Financial Services Agreement or Addendum (as applicable), the Customer can request Google's security documentation at any time and Google will cooperate with the customer's/regulator's requests.
5.9.4	An institution should ensure that these expectations are met in its outsourcing arrangements with the service provider as well as any sub-contractor that the service provider may engage in the outsourcing arrangement, including any disaster recovery and backup service providers. MAS will provide the institution reasonable notice of its intent to exercise its inspection rights and share its findings with the institution where appropriate.	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Agreement or Addendum (as applicable). Google agrees contractually with providers on adherence to Google's security and privacy policies and has a vendor audit program to determine compliance. Google does not depend on supply-chain partners for its disaster recovery and backup services.

5.9.5	An institution should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the institution should consider the nature and extent of risk and impact to the institution 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 institution's observance of these Guidelines in relation to the outsourcing arrangement.	Primarily customer responsibility to satisfy this requirement. Google Cloud undergoes several independent third-party audits on a regular basis. For each one, an independent auditor examines our data centres, infrastructure, and operations. Among our numerous third-party certifications, GCP and G Suite are certified or compliant with the following international standards particularly relevant in the Asia-Pacific region: - MTCS Singapore Standard 584, Tier 3 - ISO 27001 - ISO 27017 - ISO 27018 - SOC 1; SOC 2; and SOC 3 (SSAE 16 / ISAE 3402 Type II) For a full list of available certifications and compliance materials, please refer to https://cloud.google.com/security/compliance. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Agreement or Addendum (as applicable).
5.9.6	The independent audit and/or expert assessment on the service provider and its subcontractors may be performed by the institution's internal or external auditors, the service provider's external auditors or by agents appointed by the institution. The appointed persons should possess the requisite knowledge and skills to perform the engagement, 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. Institutions and the 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 institution 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	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Agreement or Addendum (as applicable). For a full list of available certifications and compliance materials, please refer to https://cloud.google.com/security/compliance.
5.9.7	Significant issues and concerns should be brought to the attention of the senior management of the institution and service provider, or to the institution's board, where warranted, on a timely basis. Actions should be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the institution's risk tolerance	Primarily customer responsibility to satisfy this requirement.
5.9.8	Copies of audit reports should be submitted by the institution to MAS. An institution should also, upon request, provide MAS with other reports or information on the institution and service provider that is related to the outsourcing arrangement.	Primarily customer responsibility to satisfy this requirement. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and the Financial Services Agreement or Addendum (as applicable).
5.10 - Outsourcing Outside Singapore		
Item #	**MAS Guideline Recommended Practices**	**Google Cloud Support**
5.10.1(a), (b), (c), & (d)	In its risk management of such outsourcing arrangements, an institution 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 institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.	Primarily customer responsibility to satisfy this requirement. Google provides comprehensive external documentation and white papers detailing our security infrastructure and operational model. Google also maintains an internal ISMS as a risk management framework and evidence of its effectiveness is provided via our ISO 27001 certification.

5.10.2(a), (b), & (c)	Material outsourcing arrangements 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 institution (i.e., from its books, accounts and documents) in a timely manner, in particular: (a) An institution should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements. (b) An institution 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. An institution must at least commit to retrieve information readily from the service provider should MAS request for such information. The institution should confirm in writing to MAS, that the institution has provided, in its outsourcing agreements, for MAS to have the rights of inspecting the service provider, as well as the rights of access to the institution and service provider's information, reports and findings related to the outsourcing arrangement, as set out in paragraph 5.9. (c) An institution should notify MAS if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the institution and MAS set out in paragraph 5.9, have been restricted or denied.	Primarily customer responsibility to satisfy this requirement. Customers do not need Google's assistance to port their data. Customers can export their data from G Suite using Google Takeout (https://takeout.google.com/settings/takeout). Customers can export their Google Cloud Platform data in a number of industry standard formats. Google's contractual commitments regarding audit and inspection can be found under Section 7 and 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7 and 7.5.2 of the Data Processing Amendment (DPA) for G Suite, and under the Financial Services Agreement or Addendum (as appropriate) signed between Google and the Customer.
5.11 - Outsourcing Within a Group - This section is intentionlly omitted		
5.12 - Outsourcing of Internal Audit to External Auditors - This section is intentionlly omitted		