Bank Negara - Outsourcing Policy

Google Cloud Mapping

This document is designed to help financial institutions supervised by Bank Negara ("**regulated entity**") to consider the Bank Negara Outsourcing Policy Document dated 23 October 2019 ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Section 9 - outsourcing process and management of risks, Section 10 - outsourcing outside Malaysia, Section 11 - outsourcing involving cloud services. 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.	**9**	**Outsourcing process and management of risks**		
2.	G 9.1	Effective management of outsourcing risk requires financial institutions to have an in-depth and holistic understanding of risks arising from outsourcing arrangements. This entails an understanding of the relationship between the financial institution and the service provider, and impact of the outsourcing arrangement to the operations of the financial institution.	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation.	N/A
3.	***Assessment of service provider***			
4.	G 9.2	Conducting a comprehensive and robust due diligence process is necessary for a financial institution to make an informed selection of service providers in relation to the risks associated with the outsourcing arrangement.	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.	N/A
5.	S 9.3	A financial institution must conduct appropriate due diligence of a service provider at the point of considering all new arrangements, and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process must be commensurate with the materiality of the outsourced activity. The due diligence process must cover, at a minimum -		
6.	[Footnote 12]	(a) capacity, capability, financial strength and business reputation[12] This includes an assessment that the service provider is a going concern and has strong governance structures to manage the outsourced activity throughout the duration of the arrangement.	Capacity and capability • 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 employs some of the world's foremost experts in information, application and network security. • Information about Google Cloud's leadership team is available on our Media Resources page. Financial strength • You can review Google's audited financial statements on Alphabet's Investor Relations page. Business reputation • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
7.	(b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management[13] [Footnote 13] Including the ability of the service provider to respond to service disruptions or problems resulting from natural disasters, or physical or cyber-attacks, within an appropriate timeframe.	Internal controls Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 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. Business continuity management Refer to Rows 55 to 66 for more information on business continuity.	Certifications and Audit Reports
8.	(c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites;	Information about the location of Google's facilities and where individual GCP services can be deployed is available here.	N/A
9.	(d) access rights of the financial institution and the Bank to the service provider;	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access
10.	(e) measures and processes to ensure data protection and confidentiality;	Refer to Row 46 for more information on data protection and confidentiality.	N/A
11.	(f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement;	Refer to Rows 35 to 38 for information on how Google manages subcontractors.	N/A
12.	(g) undue risks[14] resulting from similar business arrangements, if any, between the service provider and the financial institution;	Refer to Row 13 for more information on how you can manage concentration risk.	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
	[Footnote 14]	For instance, concentration risk to a systemic service provider in the industry or where the service provider's fee structure or relationship with the financial institution may create potential conflict of interest issues.		
13.	(h)	the extent of concentration risk to which the financial institution is exposed with respect to a single service provider and the mitigation measures to address this concentration. This does not apply to a service provider that is an affiliate and is supervised by a financial regulatory authority; and	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
14.	(i)	ability of the service provider to comply with relevant laws, regulations and requirements in this policy document.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. In addition, Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance.	Representations and Warranties Enabling Customer Compliance
15.	S 9.4	In performing due diligence on an affiliate, the institution must make an objective assessment of the affiliate's ability to perform the outsourced activity guided by the considerations applied in paragraph 9.3. The depth of such a due diligence process may be different if the service provider is an affiliate that is supervised by a financial regulatory authority.	This is a customer consideration.	N/A
16.	S 9.5	A financial institution must ensure that the outcomes of the due diligence process are well-documented and escalated to the board, where relevant, in line with the outsourcing risk management framework of the financial institution.	This is a customer consideration.	N/A
17.	***Outsourcing agreement***			
18.	S 9.6	An outsourcing arrangement must be governed by a written agreement that is legally enforceable. The outsourcing agreement must, at a minimum, provide for the following–	The use of the Services is governed by the Google Cloud Financial Services Contract.	N/A
19.	(a)	duration of the arrangement with date of commencement and expiry or renewal date;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
20.	(b)	responsibilities of the service provider, with well-defined and measurable risk and performance standards in relation to the outsourced activity. Commercial terms tied to the performance of the service provider must	Performance standards	Services

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	not create incentives for the service provider to take on excessive risks that would affect the financial institution;	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Commercial terms Refer to your Google Cloud Financial Services. Prices and fee information are also publicly available on our SKUs page.	Payment Terms
21.	(c) controls to ensure the security of any information shared with the service provider at all times, covering at a minimum–	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 46 for more information on Google's security practices.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
22.	(i) responsibilities of the service provider with respect to information security;	Refer to Row 46 for more information on Google's responsibilities with respect to information security.	N/A
23.	(ii) scope of information subject to security requirements;	Google's security commitments in the Cloud Data Processing Addendum apply to all customer data under your account.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
24.	(iii) provisions to compensate the financial institution for any losses and corresponding liability obligations arising from a security breach attributable to the service provider;	Refer to your Google Cloud Financial Services Contract.	Liability
25.	(iv) notification requirements in the event of a security breach; 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	Data Incidents (Cloud Data Processing Addendum)
26.	(v) applicable jurisdictional laws;	Refer to your Google Cloud Financial Services Contract.	Governing Law
27.	(d) use of information shared with the service provider is limited to the extent necessary to perform the obligations under the outsourcing agreement;	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. 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
28.	(e) continuous and complete access by the financial institution to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement;	Regulated entities may access their data on the services at any time. Refer to Row 34 for more information on how you retrieve your data on termination.	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
29.	(f)	ability of the financial institution and its external auditor [15] to conduct audits and on-site inspections on the service provider and its sub-contractors, and to obtain any report or finding made in relation to the outsourced activity; [Footnote 15] Including an agent appointed by the financial institution.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities. Refer to Row 7 for more information on the third-party reports that Google makes available.	Regulator Information, Audit and Access; Customer Information, Audit and Access Google Subcontractors
30.	(g)	notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations;	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)
31.	(h)	measures that the service provider would take to ensure continuity of the outsourced activity in the event of an operational disruption or failure on the part of the service provider;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. 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
32.	(i)	regular testing of the service provider's business continuity plans (BCP), including specific testing that may be required to support the financial institution's own BCP testing, and a summary of the test results to be provided to the financial institution with respect to the outsourced activity;	Refer to Row 31 above.	N/A
33.	(j)	the dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;	Disputes Refer to your Google Cloud Financial Services Contract. Remedies	Governing Law

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Indemnity Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Services Indemnification
34.	(k) circumstances that may lead to termination of the arrangement, the contractual parties' termination rights and a minimum period to execute the termination provisions, including providing sufficient time for an orderly transfer of the outsourced activity to the financial institution or another party;	Termination Regulated entities can elect to terminate our contract for convenience with advance notice, including for Google's material breach after a cure period. Transfer 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. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Term and Termination Transition Term Data Export (Cloud Data Processing Addendum)
35.	(l) where relevant, terms governing the ability of the primary service provider to sub-contract to other parties. Sub-contracting should not dilute the ultimate accountability of the primary service provider to the financial institution over the outsourcing arrangement, and the institution must have clear visibility over all sub-contractors[16]. Therefore, the outsourcing	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	Google Subcontractors

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		agreement between the financial institution and primary service provider must stipulate the following: [Footnote 16] In this respect, the primary service provider must provide sufficient notice to the financial institution before entering into an agreement with the sub-contractor.	• give regulated entities the ability to terminate if they have concerns about a new subcontractor.	
36.		(i) the accountability of the primary service provider over the performance and conduct of the sub-contractor in relation to the outsourcing arrangement;	Google will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
37.		(ii) the rights of the financial institution to terminate the outsourcing agreement in the event of excessive reliance on sub-contracting (e.g. where the sub-contracting materially increases the risks to the financial institution); and	Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
38.		(iii) the requirement for the sub-contractor and its staff to be bound by confidentiality provisions even after the arrangement has ceased[17]; and [Footnote 17] See paragraph 9.9(f)	Google requires our subcontractors to meet the same high standards that we do. In particular: • Google requires our subcontractors to comply with our contract with you and to only access and use your data to the extent required to perform the obligations subcontracted to them. • Google will ensure that all persons authorised to process customer data are under an obligation of confidentiality. • Google's confidentiality obligations survive expiry or termination of the contract.	Requirements for Subprocessor Engagement (Cloud Data Processing Addendum) Data Security; Access and Compliance (Cloud Data Processing Addendum) Survival
39.		(m) corresponding obligations for staff of the service provider, who are involved in the delivery of services to the financial institution's customers, to comply with similar conduct standards imposed by the Bank on the financial institution.	Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality. In addition, Google requires all its employees to comply with the Alphabet Code of Conduct.	Data Security; Access and Compliance (Cloud Data Processing Addendum)
40.	S 9.7	The outsourcing agreement must also contain provisions which–		
41.		(a) enable the Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity;	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access
42.		(b enable the Bank to conduct on-site supervision of the service provider where the Bank deems necessary;	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	Regulator Information, Audit and Access

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Customer Information, Audit and Access
43.	(c) enable the Bank to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where the Bank deems necessary; and	Refer to Row 42. Google grants information, audit and access rights to supervisory authorities, and both their appointees. This includes a third party auditor appointed by the supervisory authority.	N/A
44.	(d) allow the financial institution the right to modify or terminate the arrangement when the Bank issues a direction to the financial institution to that effect under the FSA, IFSA or DFIA, as the case may be.	Regulated entities can elect to terminate our contract for convenience with advance notice, including if directed by a supervisory authority.	Term and Termination
45.	***Protection of data confidentiality***		
46.	G 9.8 Misuse, unauthorised or inadvertent disclosure of confidential information is a serious risk event for financial institutions. It is therefore imperative that the financial institution satisfies itself that the level of security controls, governance, policies, and procedures at the service provider are robust to protect the security and confidentiality of information shared under the outsourcing arrangement.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and security of information when using 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)

Bank Negara - Outsourcing Policy

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	
47.	S 9.9 A financial institution must ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, the financial institution must ensure that–	Refer to Row 46 for more information on the security, confidentiality and integrity of data.	N/A
48.	(a) information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and 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 you provide to the services under your account.	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
49.	(b)	information shared with the service provider is used only to the extent necessary to perform the obligations under the outsourcing agreement;	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
50.	(c)	all locations (e.g. city and country) where information is processed or stored, including back-up locations, are made known to the financial institution;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available 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)
51.	(d)	where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia;	Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the Cloud Data Processing Addendum.	Representations and Warranties
52.	(e)	where the service provider provides services to multiple clients, the financial institution's information must be segregated[18] from the information of other clients of the service provider; [Footnote 18] Either logically or physically.	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)
53.	(f)	the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even after the arrangement has ceased; and	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure. Google's confidentiality obligations survive expiry or termination of the contract.	Confidentiality Survival

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
54.	(g) information shared with the service provider is destroyed, rendered unusable, or returned to the financial institution in a timely and secure manner once the outsourcing arrangement ceases or is terminated.	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 Platform whitepaper. Return Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Deletion on Termination (Cloud Data Processing Addendum) Data Export (Cloud Data Processing Addendum)
55.	***Business continuity planning***		
56.	G 9.10 A financial institution is responsible for ensuring that its BCP consider any operational disruptions at, or failure of, the service provider.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. 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
57.	S 9.11 A financial institution must ensure that its BCP provide for all outsourcing arrangements. The depth and comprehensiveness of the BCP must be commensurate with the materiality of the outsourcing arrangements. At a minimum, the financial institution must ensure that the BCP include probable, adverse scenarios[19] with specific action plans. The practicality of such plans must, among others, take into consideration– [Footnote 19] For instance, failure, liquidation or operational disruption of the service provider, non-performance by the service provider, unexpected termination of the outsourcing arrangement, or material deterioration in the performance of the service provider.	Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including destruction of infrastructure required to provide the Services, interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures), unavailability of key personnel, emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) and pandemics. We recognize that, whatever the level of technical resilience that can be achieved on GCP, regulated entities must plan for the scenario in which Google can no longer provide the service.	Business Continuity and Disaster Recovery

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference			Google Cloud commentary	Google Cloud Financial Services Contract reference
				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 GCP across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commit to open source and common standards.	Data Export (Cloud Data Processing Addendum)
58.		(a)	the estimated cost involved to resume the outsourced activity;	This is a customer consideration.	N/A
59.		(b)	the possible need for an alternative service provider, including considerations of the limited number of service providers in the market; and	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
60.		(c)	the degree of difficulty, cost and time required to reintegrate the outsourced activity in-house.	Refer to Row 59 above.	N/A
61.	S 9.12		In the event of a disruption, material outsourced activities must be resumed without undue delay and with minimal impact and disruptions to both business operations and the financial institution's customers.	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.	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications	
62.	S 9.13 A financial institution must, at all times, ensure that it has ready access to all its records and information at the service provider with respect to the outsourced activity which would be necessary for it to operate and meet its legal and regulatory obligations. This includes scenarios where network connectivity is not available, the service provider becomes insolvent or a dispute resolution process is ongoing.	You retain all intellectual property rights in your data. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: ● Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ● Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. ● You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	Intellectual Property Data Export (Cloud Data Processing Addendum) Term and Termination
63.	S9.14 A financial institution must periodically test its own BCP and proactively seek assurance on the state of BCP preparedness of the service provider and where relevant, alternative service providers. The intensity and regularity of the BCP testing and assessments of BCP preparedness must be commensurate with the materiality of the outsourcing arrangement. In assessing this preparedness, the financial institution must, at a minimum–	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.	Business Continuity and Disaster Recovery
64.	(a) ensure that the back-up arrangements are available and ready to be operated when necessary;	Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup	N/A
65.	(b) ensure that the service provider periodically tests its BCP and provides any test reports, including any identified deficiencies, that may affect the provision of the outsourced service and measures to address such deficiencies as soon as practicable; and	Refer to Row 63 above.	N/A

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
66.	(c) for material outsourcing arrangements, participate in joint testing with the service provider to enable an end-to-end BCP test for these arrangements by the financial institution.	Refer to Row 63 above.	N/A
67.	**10 Outsourcing outside Malaysia**		
68.	G 10.1 Outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia exposes a financial institution to additional risks (e.g. country risk). A financial institution should have in place appropriate controls and safeguards to manage these additional risks, having regard to social and political conditions, government policies, and legal and regulatory developments.	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. 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 Location (Service Specific Terms)
69.	S 10.2 In conducting the due diligence process, a financial institution must ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the financial institution or service provider to implement appropriate responses to emerging risk events in a timely manner.	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 Security; Subprocessors (Cloud Data Processing Addendum)
70.	S 10.3 A financial institution must ensure that outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect–		
71.	(a) the financial institution's ability to effectively monitor the service provider and execute the institution's BCP;	Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services.	Ongoing Performance Monitoring

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Business Continuity Planning Refer to Rows 55 to 66 for more information on business continuity planning.	
72.	(b) the financial institution's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. These rights apply regardless of where the data are stored. Refer to Row 62 for information on the protections that apply in the unlikely event of Google's insolvency.	Regulator Information, Audit and Access
73.	(c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity.	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
74.	**11 Outsourcing involving cloud services**		
75.	G 11.1 Where the outsourcing arrangement involves a cloud service provider, a financial institution should take effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance. This is particularly important as cloud service providers often operate a geographically dispersed computing infrastructure with regional or global distribution of data processing and storage.	This document explains how regulated entities can address their requirements whilst using Google Cloud services.	N/A
76.	S 11.2 In using cloud services, the inherent risks involved are similar to that of other forms of outsourcing arrangements. A financial institution that subscribes to cloud services must comply with the requirements of this policy document, and other relevant requirements on cloud services as specified by the Bank.	This document explains how regulated entities can address their requirements whilst using Google Cloud services.	N/A
77.	S 11.3 In relation to a financial institution's ability to conduct audits and inspections on the cloud service provider and sub-contractors pursuant to paragraph 9.6(f), the financial institution may rely on third party certification and reports made	Third-party reports	Certifications and Audit Reports

Bank Negara - Outsourcing Policy

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	available by the cloud service provider for the audit[20], provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit. [Footnote 20] For the avoidance of doubt, such certifications or reports should not substitute the financial institution's right to conduct on-site inspections where necessary.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems) ● ISO/IEC 27017:2015 (Cloud Security) ● ISO/IEC 27018:2014 (Cloud Privacy) ● PCI DSS ● SOC 1 ● SOC 2 ● SOC 3 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. Scope of audit 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. Audit right Regulated entities always retain the right to conduct an audit. Google offers regulated entities certifications and audit reports in addition to (and not instead of) audit, access and information rights.	Certifications and Audit Reports Customer Information, Audit and Access
78.	S 11.4 In relation to the testing of a cloud service provider's BCP pursuant to paragraph 9.6(i), a financial institution must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising from the BCP testing.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery