Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

This document is designed to help banks and financial institutions supervised by the Central Bank of Malaysia to consider the Risk Management in Technology (RMiT) Policy Requirements (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the standards and guidelines in Section 10 - Technology Operations Management of the framework. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	**10 Technology Operations Management**		
2	**Cryptography**		
3	S 10.16 A financial institution must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. This policy, at a minimum, shall address requirements for:		
4	(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;	Customers are responsible for adopting their cryptography policy. Meanwhile, encryption is central to Google’s comprehensive security strategy. We provide certain encryption by default, with no additional action required from you. We also offer a continuum of encryption key management options to meet your needs. Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation.	N/A
5	(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;	Refer to row 4.	N/A
6	(c) the periodic review, at least every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and	Google reviews its encryption library regularly to ensure they are current with the latest attack vectors.	N/A
7	(d) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.	Customers are responsible for developing and testing their compromise-recovery plans in the event of a cryptographic key compromise. For our part, Google stores customer data in subfile chunks that are encrypted at the storage level. Each chunk is distributed across Google’s storage systems and replicated in encrypted form for backup and disaster recovery.	N/A
8	S 10.17 A financial institution shall ensure clear senior-level roles and responsibilities are assigned for the effective implementation of the cryptographic policy.	This is a customer consideration.	N/A
9	S 10.18 A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution’s risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.	Google maintains documentation on its cryptographic controls and key management process and provides controls to manage encryption keys through their lifecycle. You can choose to use these encryption and key management tools provided by Google: • Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises • Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. • Customer-managed encryption keys for Cloud SQL and GKE persistent disks. • Cloud External Key Manager (beta) lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. • Key Access Justification (alpha) works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set. Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation. **Third party assessments** Google recognizes that you need to conduct due diligence and perform an 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	
10	S 10.19 A financial institution must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols must be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation must be undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEE).	This is a customer consideration.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
11	S 10.20 A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications.	This is a customer consideration.	N/A
12	**Data Centre Resilience**		
13	**Data Centre Infrastructure**		
14	S 10.21A financial institution must specify the resilience and availability objectives of its data centres which are aligned with its business needs.The network infrastructure must be designed to be resilient, secure and scalable. Potential data centre failures or disruptions must not significantly degrade the delivery of its financial services or impede its internal operations.	Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities 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. 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	N/A
15	S 10.22 A financial institution must ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.	All Google data centres, including the software and computer hardware, are designed and managed to be highly redundant. Refer to our Google Cloud Infrastructure page for more information.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
16	S 10.23 In addition to the requirement in paragraph 10.22, large financial institutions are also required to ensure recovery data centres are concurrently maintainable.	Refer to row 15.	N/A
17	S 10.24 A financial institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A financial institution must also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A financial institution must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues.	To keep things running 24/7 and ensure uninterrupted services, Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Refer to our data center security page along with our Google Infrastructure Security Design Overview whitepaper for more information.	N/A
18	S 10.25 A financial institution is required to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA) and set proportionate controls aligned with the financial institution's risk appetite. The assessment must consider all major risks and determine the current level of resilience of the production data centre. A financial institution must ensure the assessment is conducted at least once every three years or whenever there is a material change in the data centre infrastructure, whichever is earlier. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.22 to 10.24 have been adhered to. For data centres managed by third party service providers, a financial institution may rely on independent third party assurance reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.	Google recognizes that customers may need to review our assurance reports as part of their risk assessment. 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.	Certifications and Audit Reports
19	**Data Centre Operations**		
20	S 10.26 A financial institution must ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth. A financial institution shall involve both the technology stakeholders and the relevant business stakeholders within the financial institution in its development and implementation of capacity management plans.	When using Google Cloud services, customers hand off the bulk of their capacity planning to Google. You can scale up and scale down your VM instances as needed. In addition, customers can choose to use Cloud Load Balancing which provides scaling, high availability, and traffic management for your internet-facing and private applications. Refer to our Capacity Management with Load Balancing page for more information.	N/A
21	S 10.27 A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	Google allows customers to monitor the consumption of their services Monitoring	Ongoing Performance Management

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The Status Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
22	S 10.28 A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities.	Access and Site Controls (Cloud Data Processing Addendum)
23	S 10.29 A financial institution must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions.	Refer to our batching requests page for more information.	N/A
24	S 10.30 A financial institution is required to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times. A financial institution must also maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup media must be stored in an environmentally secure and access-controlled backup site.	Google has implemented environmental controls, backup and fall-over mechanisms, and other redundancies for all its data centres. Financial institutions 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
25	G 10.31 In regard to paragraph 10.30, a financial institution should also adopt the controls as specified in Appendix 1 or their equivalent to secure the storage and transportation of sensitive data in removable media.	This is a customer consideration.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
26	S 10.32 Where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that the relevant critical systems are designed for high availability with a cumulative unplanned downtime affecting the interface with customers or counterparties of not more than 4 hours on a rolling 12 months basis and a maximum tolerable downtime of 120 minutes per incident.	This is a customer consideration. Refer to Row 14 for more information.	N/A
27	**Network Resilience**		
28	S 10.33 A financial institution must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.	Google's network provides high performance, scale, and redundancy for customers through globally distributed entry points. Refer to our Google Cloud Infrastructure page for more information about our network resilience.	N/A
29	S 10.34 A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.	Refer to Row 28 for more information.	N/A
30	S 10.35 A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.	Refer to Row 21 for more information.	N/A
31	S 10.36 A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	Confidentiality At Google, Customer data is encrypted at rest and in transit by default in order to keep data confidential. • **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. More information on Google's security products that may help with the security and confidentiality of your workload is available on our Cloud Security Products page. Integrity Data integrity refers to the accuracy and consistency of data throughout its lifetime.	Confidentiality Data Security; Security Measures Certifications and Audit Reports (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Customers need to know that information will be correct and won't change in some unexpected way from the time it's first recorded to the last time it's observed. Given the different ways data can be lost, there is no silver bullet that guards against the many combinations of failure modes. As such, Google employs a defense in depth strategy that comprises multiple layers, with each successive layer of defense conferring protection from progressively less common data loss scenarios. More information on data integrity can be found on our Site Reliability Engineering page. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access. Google also maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use. Availability Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. In addition, Google maintains policies and procedures to ensure consideration of availability throughout the entire Customer engagement. Google provides customers with uptime availability metrics and industry standard audit reports and certifications. Google maintains a dashboard for service availability information and service issues: https://status.cloud.google.com/	
32	S 10.37 A financial institution must establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint must highlight both physical and logical connectivity between network components and network segmentations.	Refer to our Cloud networking page for information on best practices and examples to assist with networking on Google Cloud.	N/A
33	S 10.38 A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.	Customers can use device logs to find information about device connections, errors, and other lifecycle events.	N/A
34	S 10.39 A financial institution must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the financial institution from other entities within the group.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	N/A
35	S 10.40 A financial institution is required to appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and	This is a customer consideration.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the financial institution's adherence to the requirements in paragraphs 10.33 to 10.39. The designated board-level committee must deliberate the outcome of the assessment.		
36	**Third Party Service Provider Management**		
37	S 10.41 The board and senior management of the financial institution must exercise effective oversight and address associated risks when engaging third party service providers for critical technology functions and systems. Engagement of third party service providers, including engagements for independent assessments, does not in any way reduce or eliminate the principal accountabilities and responsibilities of financial institutions for the security and reliability of technology functions and systems.	This is a customer consideration.	N/A
38	S 10.42 A financial institution must conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services.	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. Reputation • Qualifications and competencies: Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Performance record: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard. Financial viability You can review information about Google's financial performance and condition on Alphabet's Investor Relations page. This provides information about our financial strength and viability.	N/A
39	In addition, an assessment shall be made of the third party service provider's capabilities in managing the following specific risks–		
40	(a) data leakage such as unauthorised disclosure of customer and counterparty information;	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. You can also monitor and control the limited actions performed by Google personnel on your data using these tools:	Access and Site Controls (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	
41	(b) service disruption including capacity performance;	Refer to Row 20 for more information on capacity performance. Google recognizes the importance of managing service disruptions. We do our own planning for our services. You can also use our services in your own business continuity and contingency planning. Google will implement a disaster recovery and business contingency plan for our services, review and test it at least annually and ensure it remains current with industry standards. Financial institutions 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 on the Google Cloud Platform Disaster Recovery Planning Guide page.	Business Continuity and Disaster Recovery
42	(c) processing errors;	Customers can use Error Reporting which aggregates and displays errors produced in your running cloud services. Using the centralized error management interface, you can find your application's top or new errors so that you can fix the root causes faster.	N/A
43	(d) physical security breaches;	Google maintains a physical security policy that describes the requirements for maintaining a safe and secure work environment. More information on Google's physical security features is available in our Google Security whitepaper.	N/A
44	(e) cyber threats;	Google provides detailed information to customers about our security practices used to stop cyber threats. 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	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
45	(f) over-reliance on key personnel;	Customers can operate the services independently without action by Google personnel. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there is no single Google personnel dedicated to delivering the services to an individual customer.	N/A
46	(g) mishandling of confidential information pertaining to the financial institution or its customers in the course of transmission, processing or storage of such information; and	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. Google personnel are trained on Google's Data Security policy including procedures for handling customer data.	Protection of Customer Data
47	(h) 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. In addition, 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.	Data Export (Cloud Data Processing Addendum)
48	S 10.43 A financial institution must establish service-level agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following:		
49	(a) access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution. This shall include access to any record, file or data of the financial institution, including management information and the minutes of all consultative and decision-making processes;	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page. Google grants audit, access and information rights to regulatory authorities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits.	Services Regulator Information, Audit and Access

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Nothing in our contract is intended to impede or inhibit the regulatory authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help regulatory authorities review our Services, our contract does not contain caveats or pre-defined steps before regulatory authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services. Google will cooperate with regulatory authorities exercising their audit, access and information rights. Google recognizes that using our Services should not impair a financial institution's (or their regulator's ability) to oversee and supervise compliance with applicable laws and regulations as well as a financial institution's internal policies. We will provide financial institutions with the assistance they need to review our Services.	Enabling Customer Compliance
50	(b) requirements for the service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial;	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor. To enable financial institutions to retain oversight of any sub-outsourcing and provide choices about the services financial institutions use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give financial institutions the ability to terminate if they have concerns about a new subcontractor. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. In particular, we recognize that sub-outsourcing must not reduce financial institutions' ability to oversee the service or the regulators' ability to supervise the financial institution. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to financial institutions and their regulators. Refer to Google Cloud Platform Subprocessors for a list of our subprocessors.	Google Subcontractors
51	(c) a written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall further clearly provide for the service provider	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended;	Google will comply with all laws and regulations applicable to it in the provision of the Services.	Representations and Warranties
52	(d) arrangements for disaster recovery and backup capability, where applicable;	Refer to Row 41 for information on Google's ability to provide disaster recovery and business continuity.	N/A
53	(e) critical system availability; and	The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.	Services
54	(f) arrangements to secure business continuity in the event of exit or termination of the service provider.	Google recognizes that financial institutions 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 financial institutions achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a financial institution would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services. 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.	Transition Term Transition Assistance
55	S 10.44 A financial institution must ensure its ability to regularly review the SLA with its third party service providers to take into account the latest security and technological developments in relation to the services provided.	Financial institutions can review Google's SLAs on our Google Cloud Platform Service Level Agreements page.	Services
56	S 10.45 A financial institution must ensure its third party service providers comply with all relevant regulatory requirements prescribed in this policy document.	Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services.	Representations and Warranties
57	S 10.46 A financial institution must ensure data residing in third party service providers are recoverable in a timely manner. The financial institution shall ensure clearly defined arrangements with the third party service provider are in place to facilitate the financial	Significant Developments Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page.	Data Incidents (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	institution's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.	Security Breaches 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.	
58	S 10.47 A financial institution must ensure the storage of its data is at least logically segregated from the other clients of the third party service provider. There shall be proper controls over and periodic review of the access provided to authorised users.	Refer to Row 34.	N/A
59	S 10.48 A financial institution must ensure any critical system hosted by third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service provider.	Refer to Row 41 for information on Google's ability to provide disaster recovery and business continuity. Refer to Row 54 for more information about how our Services support exit.	N/A
60	**Cloud Services**		
61	S 10.49 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet.	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
62	The assessment must specifically address risks associated with the following:		
63	(a) sophistication of the deployment model;	The GCP services are described on our services summary page. Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.	Definitions
64	(b) migration of existing systems to cloud infrastructure;	Our Services enable you to transfer your data independently. If a financial institution would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance
65	(c) location of cloud infrastructure;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available here. • Information about the location of Google's subprocessors' facilities is available here. Google provides the same contractual commitments and technical and organizational	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Processing Addendum) Data Location (Service Specific Terms)
66	(d) multi-tenancy or data co-mingling;	Refer to Row 34.	N/A
67	(e) vendor lock-in and application portability or interoperability;	Refer to Row 47.	N/A
68	(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;	Google maintains security configurations for its machines and network devices	N/A
69	(g) exposure to cyber-attacks via cloud service providers;	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. This is described in the Cloud Data Processing Addendum. 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. Refer to row 6.	Data Security; Security Measures (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. ● **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (b) Security products 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	
70	(h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination;	Refer to Row 54 for information about how our Services support exit. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Deletion on Termination (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
71	(i) demarcation of responsibilities, limitations and liability of the service provider; and	The rights and responsibilities obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
72	(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.	Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services.	Representations and Warranties
73	S 10.50 A financial institution must separately identify critical and non-critical systems prior to using any cloud services, guided by the definition of “critical system” in paragraph 5.2. A financial institution must notify the Bank of its intention to use cloud services for non-critical systems. The risk assessment as outlined in paragraph 10.49 must be documented and made available for the Bank’s review as and when requested by the Bank.	This is a customer consideration.	N/A
74	S 10.51 A financial institution is required to consult the Bank prior to the use of public cloud for critical systems. The financial institution is expected to demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in paragraph 10.49 as well as the following areas:		
75	(a) the adequacy of the over-arching cloud adoption strategy of the financial institution including: (i) board oversight over cloud strategy and cloud operational management; (ii) senior management roles and responsibilities on cloud management; (iii) conduct of day-to-day operational management functions; (iv) management and oversight by the financial institution of cloud service providers; (v) quality of risk management and internal control functions; and (vi) strength of in-house competency and experience;	This is a customer consideration.	N/A
76	(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas: (i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and (ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit; and	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Refer to Row 18 on the third party audit reports we maintain.	N/A
77	(c) the degree to which the selected cloud configuration adequately addresses the following attributes: (i) geographical redundancy; (ii) high availability; (iii) scalability; (iv) portability; (v) interoperability; and	Refer to Row 41 for information on Google’s ability to provide disaster recovery and business continuity. Refer to Row 54 for information on Google’s efforts to enable you to access and export your data throughout the duration of our contract.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	(vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.		
78	S 10.52 A financial institution shall consider the need for a third party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 10.51.	This is a customer consideration.	N/A
79	S 10.53 A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services, and your applications. Use of your information You can provide Google instructions about your data and Google will comply with those instructions. 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.	Intellectual Property Protection of Customer Data
80	**Access Control**		
81	S 10.54 A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention. Google will ensure its employees comply with Google's security measures. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. There are a number of ways to integrate our services with your systems and to perform effective access management. **Integration** • Cloud Console allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage. • Cloud APIs allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. **Access management**	Access and Site Controls (Cloud Data Processing Addendum)

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. • Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.	
82	G 10.55 In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy:		
83	(a) adopt a “deny all” access control policy for users by default unless explicitly authorised;	Google restricts access based on need-to-know and job function.For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes.	Access and Site Controls (Cloud Data Processing Addendum)
84	(b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	Refer to Row 83.	N/A
85	(c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers;	Refer Row 83.	N/A
86	(d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as: (i) system development and technology operations; (ii) security administration and system administration; and (iii) network operation and network security;	Refer to Row 45.	N/A
87	(e) employ dual control functions which require two or more persons to execute an activity;	Refer to Row 45.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
88	(f) adopt stronger authentication for critical activities including for remote access;	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. • **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • **Cloud Audit Logs** help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. • **Multi-Factor Authentication** provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • **Access Approval** is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	N/A
89	(g) limit and control the use of the same user ID for multiple concurrent sessions;	Customers can utilize Cloud Run to manage concurrency settings.	N/A
90	(h) limit and control the sharing of user ID and passwords across multiple users; and	Google native authentication requires a minimum 8 character complex password. Financial institutions can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the financial institution who can decide to force a password change on any user that is later detected to have a password that is weak or the same as other users.	N/A
91	(i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.	Refer to Row 90.	N/A
92	S 10.56 A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate	Refer to Row 88.	N/A

Central Bank of Malaysia Risk Management in Technology

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).	Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Refer to our Multi-Factor Authentication page for more information.	
93	S 10.57 A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created.	Refer to Row 90.	N/A
94	G 10.58 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	Refer to Row 92.	N/A
95	G 10.59 A financial institution is encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.	This is a customer consideration.	N/A
96	S 10.60 A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.	Refer to Row 81.	N/A
97	S 10.61 A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams, and we provide audit logs to customers through Access Transparency for GCP.	N/A
98	S 10.62 In fulfilling the requirement under paragraph 10.61, large financial institutions are required to—		
99	(a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and	Refer to Row 81.	N/A
100	(b) deploy automated audit tools to flag any anomalies.	Refer to Row 81.	N/A