HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

This document is designed to help authorised institutions supervised by the Hong Kong Monetary Authority ("**regulated entity**") to consider TM-G-1: General Principles for Technology Risk Management ("**framework**") in the context of Google Cloud.

We focus on Section 3.1.3 - Section 7.1.1 of TM-G-1 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
1	3.1.3 Protection of information confidentiality should be in place regardless of the media (including paper and electronic media) in which the information is maintained. AIs should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud 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.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		(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 (3) Data deletion Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centres. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorised by appropriate operations manager before release. For more information, please see: https://cloud.google. com/security/deletion. Google describes its logical deletion methods in the security whitepaper below. Overwriting or cryptographic erasure are the 2 methods used for rendering information unreadable, depending on the product. https://cloud.google. com/security/deletion. As outlined in the paper above, Google has data destruction guidelines and a media erase policy which are both reviewed and updated at least annually.
2	3.1.4 If cryptographic technology is used to protect the confidentiality and integrity of AIs' information, AIs should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include:	
3	• provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorised disclosure. In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and	Google has established policies and procedures that govern the use of cryptographic controls. Google has an established key management process in place to support the organisation's use of cryptographic techniques. In addition, Google uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys. Google's cryptography policy includes guidance on the rotation of keys at regular intervals automatically. This policy also includes requirements on key rotation in case of compromise or other security issues.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Google uses a proprietary Key Management Service for storage of cryptographic keys and secrets. Google also maintains guidelines on key/secret storage. The existence and operating effectiveness of Google's encryption and key management, is verified as part of our SOC 2 audit report.
4	• adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.	Google's geographically dispersed storage services provide replication to backup system software and data so that user data is written to at least two other clusters. A combination of synchronous and asynchronous replication methods are used. Google's backup data is subject to the same logical and physical security controls as other data to protect the confidentiality, availability, and integrity of data. Google's highly available solution is discussed in the security whitepaper: https://cloud.google. com/security/overview/whitepaper. In addition, Google's KMS implementation is designed from the ground up to be resilient to outages due to their regional distribution and the ability to perform cryptographic tasks even when the entire region or zone is down.
5	3.2.1 Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine what application functions, system resources and data a user can access. For each application system, all users should be identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to ensure accountability for their activities.	Google has identity and access management policies and procedures in place. Google restricts access based on need-to-know and job function. Google also discusses administrative access in the security whitepaper: https://cloud.google. com/security/overview/whitepaper. In addition, Google has processes in place which define the steps of user access provisioning. For Google personnel, authorization is required prior to access being granted. Google maintains automated log collection and analysis tools. All account actions are recorded. Google monitors its access lists carefully to minimise the potential for unauthorised account use. Google periodically reviews access lists and removes access that is no longer required. This system automatically updates group memberships based on continuous syncs with HR data to check for changes in roles or terminations. Customers can use IAM to manage access within their system. IAM lets customers adopt the security principle of least privilege, which states that nobody should have more permissions than they actually need. With IAM, customers manage access control by defining who (identity) has what access (role) for which resource. For example, Compute Engine virtual machine instances, Google Kubernetes Engine (GKE) clusters, and Cloud Storage buckets are all Google Cloud resources. The organisations, folders, and projects that you use to organise your resources are also resources.
6	3.2.3 Extra care should be exercised when controlling the use of and access to privileged and emergency IDs. The necessary control procedures include:	
7	• granting of authorities that are strictly necessary to privileged and emergency IDs; • formal approval by appropriate personnel prior to being released for usage; • monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs); • proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data centre); and	See row 5 above. In addition, Google restricts physical and logical access to audit logs to authorised users only through the use of access control lists within the logging system. Audit information is protected from unauthorised modification and deletion through the use of checksums. Google maintains an automated log collection and analysis tool to review and analyse log events. Google also maintains policies on log retention and log security requirements.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
	• change of privileged and emergency IDs' passwords immediately upon return by the requesters.	
8	3.3.1 A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorised activities. In particular, the function should cover the following areas:	
9	• granting, changing and removing user access rights subject to proper approval of the information owners. In particular, proper procedures should be in place to ensure that a user's relevant access rights are removed when he leaves the AI or when his job responsibilities no longer require such rights;	Google maintains personnel and data access policies that govern the administration of access controls including transfers and terminations. Additionally, Google removes access to corporate assets in a timely basis upon submission of a termination request.
10	• ensuring the performance of periodic user access re-certification (e.g. on an annual basis) that confirms whether user access rights remain appropriate and obsolete user accounts have been removed from the systems;	Google maintains formal policies for the registration and de-registration of user access. The re-certification process is typically performed on an annual basis, but can be performed more frequently if necessary. The process typically involves the following steps: 1. The user's manager reviews the user's access rights and determines whether they are still appropriate. 2. If the user's access rights are no longer appropriate, the manager revokes them. 3. If the user's account is no longer needed, it is deleted.
11	• reviewing security logs and violation reports in a timely manner; and	Google maintains a central identity and authorization management system. Google requires access reviews of its security logs at least semi-annually for critical access groups.
12	• performing incident analysis, reporting and investigation.	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. These procedures include roles and responsibilities along with stakeholders who may be impacted. Google also has a data incident response whitepaper: https://cloud.google. com/security/incident-response
13	3.3.2 Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorised activities being performed by the security administration function.	Google maintains a separation of duties matrix to document the organisational roles established within the organisation. Various roles within the matrix are responsible for administrative data access, encryption, key management, and logging. Google employs the principle of least privilege, allowing only authorised access for users necessary to accomplish their job functions
14	3.3.3 AIs should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours. The incident response and reporting procedures should include timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches.	See row 12 above. Google notifies customers of data incidents promptly and without undue delay. Notification is provided to an email address designated by the customer. Customers can choose to use Essential Contacts: https://cloud.google.com/resource-manager/docs/managing-notification-contacts. More information on Google's data incident response process is available in our Data incident response whitepaper and the Cloud Data Processing Addendum. https://services.google.com/fh/files/misc/data_incident_response_2018.pdf; https://cloud.google.com/terms/data-processing-addendum. In addition, customers can leverage the below incident response tools below offered by Google Cloud: • The Google Cloud Service Health Dashboard (https://status.cloud.google.com/) shows incidents that affect many customers. When a relevant Google Cloud product or service reports an issue in the dashboard, customers may also see an outage notice in the Google Cloud console. Customers can also choose to

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		build integration to consume the information displayed on the dashboard programmatically e.g. through an RSS feed. • The Google Cloud Support Center (https://support.cloud.google.com/portal/) displays known issues. This is the most comprehensive view of issues, and includes issues that affect fewer customers than are shown on the dashboard. Customers can create a support case from a posted incident on the known issue page so that they get regular updates. • Google offers Threat Horizons intelligence reports to help keep your organisation on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat. Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud Platform Services, via https://cloud.google.com/support/bulletins
15	3.4.1 Control procedures and baseline security requirements should be developed to safeguard application programs, operating systems, system software and databases. For example:	
16	• access to data and programs should be controlled by appropriate methods of identification and authentication of users together with proper authorization;	See rows 5 and 9 above.
17	• integrity of static data (e.g. system parameters) should be periodically checked to detect unauthorised changes;	Google maintains configuration management tools to detect and automatically correct deviations from its baseline configuration and collects and secures audit records. In addition, Google has change management policies and procedures in place to restrict unauthorised changes to Google's applications, services, and systems.
18	• operating systems, system software, databases and servers should be securely configured to meet the intended uses with all unnecessary services and programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers;	See row 1 above. In addition, Google provides security best practices to all customers to help configure their environments. https://cloud.google.com/security/best-practices Google Cloud - Externally provided (CIS): • Google Cloud Foundational Benchmark checklists are made available by CIS. https://ncp.nist.gov/checklist/870. https://www.cisecurity.org/benchmark/google_cloud_computing_platform
19	• clear responsibilities should be established to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified, assessed, tested and applied to the systems in a timely manner;	Google has guidelines to perform fuzz testing, sandboxing, third-party library monitoring, source code analysis, and vulnerability scanning to detect, mitigate, and resolve security issues as part of the software testing lifecycle. Google engineering's continuous build system utilises an automated testing platform which runs tests automatically at every changelist. Google has also implemented a vulnerability management program to detect and remediate system vulnerabilities in accordance with established benchmarks. Google also performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google has a team dedicated to automated vulnerability management. Vulnerability management is also discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Customers are responsible for remediation of application security vulnerabilities (including establishing automated remediation capabilities when possible) within customer's GCP instance.
20	• all configurations and settings of operating systems, system software, databases and servers should be adequately documented. Periodic certifications of the security settings should be performed (e.g. by the TRM function or the technology audit function); and	Google develops, documents, and maintains under configuration control a current baseline for all machines and network device hardware. Google Cloud products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. Google has also created resource documents and mappings for compliance support when formal certifications or attestations may not be required or applied. Details: https://cloud.google.com/security/compliance Reports: https://cloud.google.com/security/compliance/compliance-reports-manager
21	• adequate logging and monitoring of system and user activities should be in place to detect anomalies, and the logs should be securely protected from manipulation.	Google uses a proprietary event management tool to identify and alert on atypical activity and takes timely appropriate action when unauthorised use is detected. This is done through Google's automated log collection and analysis tool, which reviews and analyses log events. Google also maintains policies on log retention and log security requirements. Customers are responsible for managing their own audit log security and retention within their GCP instance.
22	3.5.2 Controls over mobile computing are required to manage the risks of working in an unprotected environment. In protecting AIs' information, AIs should establish control procedures covering:	
23	• use of data encryption software to protect sensitive information and business transactions in the mobile environment and when being transmitted	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. Google has a security whitepaper on encryption in transit: https://cloud. google.com/security/encryption-intransit/. Customers are responsible for using secure and encrypted communication channels including up to date and approved protocols when migrating servers, services, applications, or data to cloud environments within customer managed systems and networks. In addition, Google offers Cloud Identity device management which lets customers manage company-owned and employee-owned (BYOD) devices.
24	3.6.1 Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities.	Google Data centres maintain secure external perimeter protections. All data centres employ electronic card key access control system that are linked to a system alarm. Only authorised employees, contractors, and visitors are allowed entry to the data centres. Only authorised employees and contractors are permitted to request (which is followed by proper approval process) electronic card key access to these facilities. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorised activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorised access throughout the business operations and data centres is restricted based on an individual's job responsibilities. The fire doors at the data centres are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		outside the data centres. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. Google logs all physical access of its data centre employees and retains them according to Google's retention policy.
25	3.6.2 AIs should consider fully the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of their data centers. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could affect adversely the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator.	Google has processes in place during data centre design to consider security and environmental factors when determining locations for critical rooms and equipment floor plans within the data centre. Google carefully selects the locations of its data centres to avoid exposure to high-impact environmental risks to the extent possible. Information about the location of Google's facilities and where individual Google Cloud services can be deployed, including in which region, is available at our Global Locations page (https://cloud.google.com/about/locations/). Google also has mechanisms in place to address utility outages through the implementation of a primary and alternative power source, each with equal power, for every critical component. Diesel engine backup generators can provide enough emergency electrical power to run each data centre at full capacity. Processes are tested as part of annual disaster recovery testing. Google's security whitepaper explains the redundancy of our data centres in more detail: https://cloud.google. com/security/overview/whitepaper. In addition, Google has mechanisms in place to monitor and maintain data centre temperatures and humidity through the use of smart temperature controls and "free-cooling" techniques like using outside air or reused water for cooling. Cooling systems maintain a constant operating temperature for servers and other hardware. Processes are tested as part of annual disaster recovery testing. Google's security whitepaper explains the environmental impact of our data centres in more detail: https://cloud.google. com/security/overview/whitepaper.
26	3.6.3 In controlling access by third-party personnel (e.g. service providers) to secure areas, proper approval of access should be required and their activities should be closely monitored. It is also important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for recruitment of permanent and temporary technology staff, and contractors.	Google has implemented data protection agreements required to be signed by supply chain CSPs to comply with privacy, security, access control, audit, personnel policy, SLA, and confidentiality commitments. Google vendor managers also perform quarterly performance reviews based on the agreements outlined in the vendor's service agreements. In addition, Google has a well defined vendor management policy and process to select and monitor third party providers. Google has a dedicated team to conduct ongoing audits of subprocessors for compliance. Google conducts annual reviews and audits of its subprocessors to validate adherence with Google's security requirements to ensure they provide a level of privacy and security appropriate to their access to data and the scope of the services. Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. We require our subcontractors/subprocessors to conduct similar checks on their personnel.
27	4.2.5 Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. As inappropriate handling of software licences may expose AIs to a significant risk of patent infringement, and financial and reputation losses, AIs should establish a formal software package acquisition process. In particular, the process should involve detailed evaluation of the software package (e.g. in terms of software licence, functionality, system performance and security requirements) and its supplier (e.g. its financial condition, reputation and technical capabilities).	The GCP services are described on our services summary page. Google Cloud products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. Google has also created resource documents and mappings for compliance support when formal certifications or attestations may not be required or applied. Details: https://cloud.google.com/security/compliance Reports: https://cloud.google.com/security/compliance/compliance-reports-manager.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		In addition, Google recognizes that customers need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist customers, we've provided the information below. Technical capacity / service delivery / reputation Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. You can review information about Google's historic performance of the services on our Google Cloud Service Health Dashboard. Corporate information Information about Google Cloud's corporate history is available on Alphabet's Investor Relations page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organisational policies e.g. our Code of Conduct. You can review Google's audited financial statements on Alphabet's Investor Relations page. You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct. People Information about Google Cloud's leadership team is available on our Media Resources page. Risks

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page. Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page.
28	4.2.6 AIs should ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts. For mission-critical software packages, AIs may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of the software packages under certain circumstances, such as when the software vendors cease their business.	The support services are described on our Technical Support Services Guidelines page. 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.
29	4.3.1 Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. An effective change management process helps to ensure the integrity and reliability of the production environment. AIs should develop a formal change management process that includes:	
30	• classification and prioritisation of changes and determination of the impact of changes;	Google maintains policies and procedures on data classification, protection, and handling throughout its lifecycle according to legal and regulatory requirements.
31	• roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;	Google utilises peer review to meet the goal of segregation of duties, with reviews, comments, and approvals captured in the team's development platform as part of the development process. We also employ continuous testing, continuous integration, and comprehensive monitoring and observability to rapidly detect, prevent, and correct bad changes.
32	• program version controls and audit trails;	Google has established change management policies and procedures which integrate the risk management process with the change management process. Google's change management process requires approvals from relevant stakeholders before being released into production. Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. Google has processes in place to review Security & Privacy policies annually. The policies for change management fall under this category.
33	• scheduling, tracking, monitoring and implementation of changes to minimise business disruption;	Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). In addition, Google develops, documents, and maintains a current baseline

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		for all machines and network device hardware. System changes are code reviewed by a separate technical resource to evaluate quality and accuracy of changes.
34	• a process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and	Google has processes in place to roll back changes or manage operational impact in case the changes have an adverse impact on the production environment.
35	• a post implementation verification of the changes made (e.g. by checking the versions of major amendments).	Post implementation verification process is an important part of Google Cloud's change management process. The post implementation verification process typically includes the following steps: 1. Review of the change request: The change request is reviewed to ensure that it was properly documented and that all of the required information is present. 2. Verification of the change: The change is verified to ensure that it has been implemented correctly. This may involve testing the change, reviewing documentation, or interviewing users. 3. Evaluation of the change: The change is evaluated to determine whether it is meeting the desired outcomes. This may involve collecting feedback from users, reviewing metrics, or conducting surveys.
36	4.3.2 To enable unforeseen problems to be addressed in a timely and controlled manner, AIs should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day)	Google's change management policies and procedures include an exception process for relevant use cases which require approvals, and an emergency process to be used by authorised personnel only which require emergency changes and tests to be reviewed in a timely manner.
37	4.3.3 Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.	See rows 34-40 above.
38	5.1.1 Management of IT functions should ideally formulate a service level agreement with business units to cover system availability and performance requirements, capacity for growth, and the level of support provided to users. The responsible IT functions should ensure that adequate procedures are in place for managing the delivery of the agreed technology support and services.	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. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.
39	5.1.2 Detailed operational instructions such as computer operator tasks, and job scheduling and execution (e.g. instructions for processing information, scheduling requirements and system housekeeping activities) should be documented in an IT operations manual. The IT operations manual should also cover the procedures and requirements for on-site and off-site back-up of data and software in both the production and development environments (e.g. the frequency, scope and retention periods of back-up).	Each product team at Google has a set of operating procedures, which are available to authorised personnel. Overall, Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle).
40	5.1.3 AIs should have in place a problem management system to respond promptly to IT operational incidents, to escalate reported incidents to relevant IT management staff and to record, analyse and keep track of all these incidents until rectification of the incidents. A helpdesk function can be set up to provide front-line support to users on all technology-related problems and to relay the problems to relevant IT functions for investigation and resolution.	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. This includes the use of forensics in the resolution process. Google also has a data incident response whitepaper: https://cloud.google. com/security/incident-response. To assist customers with their own incident response, Google's notification will describe:

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		• the nature of the Data Incident including the Customer resources impacted; • the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; • the measures, if any, Google recommends that Customer take to address the Data Incident; and -details of a contact point where more information can be obtained. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Autonomic Security Operations (ASO) solution: • delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defences together. • enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. Here are some examples: • Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. • Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. • Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.
41	5.3.1 To ensure the continued availability of AIs' technology-related services, AIs should maintain and service IT facilities and equipment (e.g. computer hardware, network devices, electrical power distribution, UPS and air conditioning units) in accordance with the industry practice, and suppliers' recommended service intervals and specifications. Proper record keeping (including suspected or actual faults, and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance. A hardware and facility inventory should be kept to control and track all hardware and software purchased and leased. These records can also be used for regular inventory taking.	Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centres. This includes continuously monitoring equipment performance and conducting routine preventative and regular maintenance according to organisational requirements. Customers can also leverage Cloud Asset Inventory to view, monitor, and analyse all their GCP and Anthos assets across projects and services. Not only can customers export a snapshot of their entire inventory at any point of time, they can also get real-time notifications on asset configuration changes.
42	5.4.1 AIs should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. Please refer to TM-G-2 "Business Continuity Planning" on how to develop detailed recovery procedures of application systems and technology services, and ensure adequate insurance coverage of IT resources.	Google implements a business continuity plan for our Services, reviews and tests it at least annually and ensures it remains current with industry standards. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide https://cloud.google.com/solutions/dr-scenarios-planning- guide. Google's business and systems resilience policy is reviewed annually. Google's management console provides centralised management capabilities for the Google Cloud Backup and DR Service. From the management console, customers can manage backup/recovery appliances and perform day-to-day operations. Backup/recovery appliances allow replicating data between any two appliances.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Mores specifically, from the management console, customers can: • Perform an at-a-glance, aggregated view of backup/recovery appliance health and resource utilisation through the dashboard for all managed appliances. • Discover and manage applications using the Onboarding Wizard. • Manage backup/recovery appliances through the Manage tab, create organisations and assign resources, create roles, and create users and assign roles. In addition, customers create and manage storage pools. • Configure backup plans to define how long to retain the data. • Mount backup images of Compute Engine instances. • Monitor backup/recovery appliance health and system performance in real-time with the monitor. • View reports about jobs, backup plan compliance, resource utilisation, and audit reports. https://cloud.google.com/backup-disaster-recovery/docs/concepts/introduction
43	6.1.1 Communications networks convey information and provide a channel of access to application systems and systems resources. Given their technical complexity, communications networks can be highly vulnerable to disruption and abuse. Safeguarding communications networks requires robust network design, well-defined network services and sound discipline to be observed in managing networks.	Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. At Google we rely on a zero trust system known as BeyondCorp, to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our What is Zero Trust Identity Security? blog post. In addition, Google encrypts data-in-transit at several levels. All data is encrypted while it is “in transit”, travelling over the Internet and across the Google network between data centres. See the Google Cloud Encryption in Transit page for more information. https://cloud.google.com/docs/security/encryption-in-transit Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: 1. Tightly controlling the size and make-up of Google’s attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations. Please review https://cloud.google. com/security/infrastructure/design/ regarding defence-in-depth techniques deployed across our infrastructure. 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
44	6.1.2 Overall responsibility for network management should be clearly assigned to individuals who are equipped with the know-how, skills and resources to fulfill their duties. Network standards, design, diagrams and operating procedures should be formally documented, kept up-to-date, communicated to all relevant network staff and reviewed periodically.	Google has internal teams tasked with the responsibility of monitoring, maintaining, managing, and securing the network. Customers can also view metrics and details of network traffic to other Shared VPC networks and inter-region traffic. Network Topology combines configuration information with real-time operational data in a single view. With Network Topology, customers can collect real-time telemetry and configuration data from Google's

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		infrastructure to visualise their resources. https://cloud.google.com/network-intelligence-center/docs/network-topology/concepts/overview
45	6.1.3 Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimised by automatic re-routing of communications through alternate routes should critical nodes or links fail (e.g. routing critical links to more than one external exchange or switching centre, and prearranging services with alternate telecommunications service providers).	Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimise the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper Customers are also able to configure their Cloud Architecture to achieve HA and DR mode HA: Design a multi-zone architecture with failover for high availability Make your application resilient to zonal failures by architecting it to use pools of resources distributed across multiple zones, with data replication, load balancing and automated failover between zones. Run zonal replicas of every layer of the application stack, and eliminate all cross-zone dependencies in the architecture. https://cloud.google.com/architecture/framework/reliability/design-scale-high-availability#design_a_multi-zone_architecture_with_failover_for_high_availability DR: Replicate data across regions for disaster recovery Replicate or archive data to a remote region to enable disaster recovery in the event of a regional outage or data loss. When replication is used, recovery is quicker because storage systems in the remote region already have data that is almost up to date, aside from the possible loss of a small amount of data due to replication delay. When you use periodic archiving instead of continuous replication, disaster recovery involves restoring data from backups or archives in a new region. This procedure usually results in longer service downtime than activating a continuously updated database replica and could involve more data loss due to the time gap between consecutive backup operations. Whichever approach is used, the entire application stack must be redeployed and started up in the new region, and the service will be unavailable while this is happening. For a detailed discussion of disaster recovery concepts and techniques, see Architecting disaster recovery for cloud infrastructure outages. https://cloud.google.com/architecture/framework/reliability/design-scale-high-availability#replicate_data_across_regions_for_disaster_recovery
46	6.1.4 The network should be monitored on a continuous basis. This would reduce the likelihood of network traffic overload and detect network intrusions. Monitoring activities include:	
47	• monitoring network services and performance against pre-defined targets;	Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Please review https://cloud.google. com/security/infrastructure/design/ regarding defence-in-depth techniques deployed across our infrastructure.
48	• reviewing volumes of network traffic, utilisation of network facilities and any potential bottlenecks or overloads; and	Google has procedures in place to monitor inbound and outbound communications traffic for unusual or unauthorised activities or conditions. The border router ACL is used to filter communications to only those requests that are defined as authorised activities or conditions. Load balancers act as a gateway between production machines and the outside world. Because it is possible for unusual and/or unauthorised activities to be included in permitted communications, additional security layers are implemented to protect against and monitor these situations.
49	• detection of unusual network activities based on common attack characteristics.	See rows 46 - 48 above.
50	6.1.5 Powerful network analysis and monitoring tools, such as protocol analysers, network scanning and sniffer tools, are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage (e.g. viewing of unencrypted sensitive information). The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.	See rows 43 - 49 above.
51	6.2.1 To prevent insecure connections to an AI's network, procedures concerning the use of networks and network services need to be established and enforced. These should cover:	
52	• the available networks and network services; • authorization procedures for determining who is allowed to access particular networks and network services; and • controls and procedures to protect access to network access points, network connections and network services.	Google has procedures in place to detect attempts and prevent connections to network connections by unauthorised devices. A dedicated team is responsible for managing and securing the network. In addition, Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process your data. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information.
53	6.2.2 AIs should consider segregating internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. For instance, the production systems should be located in dedicated network segments separated from other segments so that production network traffic is segregated from other traffic (e.g. connections to the internet, extranet connections to external parties and market data feeds). Sensitive data traffic between different network segments should be properly controlled and protected from being tampered with.	See row 52 above.

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
54	6.2.3 Regular reviews of the security parameter settings of network devices such as routers, firewalls and network servers are required to ensure that they remain current. Audit trails of daily activities in critical network devices should be maintained and reviewed regularly. Network operational personnel should be alerted on a real-time basis to potential security breaches.	See rows 43 - 49 above.
55	6.2.4 Network certification should be conducted when requesting local area network (LAN)/wide area network (WAN) additions or changes to AIs' corporate network. The additions or changes cover dial-in/out ports, switches, terminal servers, gateways/servers, routers, extranets and the public internet. The network certification process includes gathering data about the network environment, analysing any points of vulnerability and associated controls, and documenting whether approval is given or what additional controls are required for approval of connectivity.	See rows 43 - 49 above. Changes to network configurations are reviewed and approved prior to deployment.
56	6.3.1 If wireless local area networks (WLANs) are to be deployed, AIs should develop policies and procedures for approval, installation, operation and administration of WLANs. A risk assessment process for evaluating the sensitivity of information to be accessible via a WLAN should be formulated before a WLAN can be implemented. AIs should also develop a standard security configuration for WLAN products and follow the network certification process to ensure that WLANs are implemented in a secure manner so that they do not expose the corporate network to unmanaged risks.	See rows 43 - 49 above.
57	6.3.2 Additional security measures may be needed between the wireless workstations and the wired network to provide stronger encryption and mutual authentication. WLANs should be segregated from the corporate network (e.g. by firewalls) to prevent any unauthorised access to the corporate network via WLANs.	See rows 43 - 49 above.
58	7.1.1 While AIs are expected to take into account the general guidance specified in SA-2 "Outsourcing" when managing technology outsourcing, they should also have regard to the following controls:	
59	• technology service providers should have sufficient resources and expertise to comply with the substance of the AIs' IT control policies;	See row 27 above.
60	• in case of outsourcing of critical technology services (e.g. data centre operations), AIs are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider. The independent assessment report should set out clearly the objectives, scope and results of the assessment and should be provided to the HKMA for reference;	Google recognizes that customers 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 customers: • 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 • CSA STAR • BSI C5:2020

HKMA General Principles for Technology Risk Management (TM-G-1)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary
		Customers can review Google's current certifications, including related evidences or reports, at any time. https://cloud.google.com/security/compliance/offerings/#/ Customers can also access the compliance reports manager, which provides an easy, on-demand access to these critical compliance resources. https://cloud.google.com/security/compliance/compliance-reports-manager
63	• the outsourcing agreement should specify clearly, among other things, the performance standards and other obligations of the technology service provider, and the issue of software and hardware ownership. As technology service providers may further sub-contract their services to other parties, AIs should consider including a notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services;	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organisation is ultimately accountable for, such as physical security of our data centres. It is important for customers to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organisation and the cloud service provider. Responsibility in the cloud is assigned as follows: Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. Customers retain all intellectual property rights in their data, the data they derive from their data using our services and their applications. Your organisation is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers. Google 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 also ensure its subcontractors comply with Google's security measures and that all persons authorised to process customer data are under an obligation of confidentiality.
64	• further to the regular monitoring activities set out in SA-2 "Outsourcing", AIs should conduct an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services;	See row 62 above. Google recognizes that customers must be able to audit our services effectively. Google grants such information, audit and access rights to customers.