Cloud service provider disclosure (MTCS SS584:2020)

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Date of Disclosure: 2024-04-11

Applicable cloud service(s): Google Cloud Services

Cloud Service Provider Contact Information

Company name: Google LLC

Primary address:

1600 Amphitheatre Parkway

Mountain View, California 94043, United States

Web address: https://cloud.google.com

Contact name: John Mulder, Director, Compliance Assurance and Audit

Contact number: +1 (212) 565 - 7927 Contact email: jmulder-mtcs@google.com

MTCS Certificate Number: GCP 2018-014 / Workspace 2018-015

Company Chop GOOGLE LLC CORPORATE SEAL 2017 DELAWARE Company Representative Signature: DocuSigned by: J.A. Mulder CFC7CB9F1AAF4C6...

Certification Body Contact Information

Company name: _____

Web address: _____

Contact name: _____

Contact number: _____ Contact email: _____

Company Chop: _____ Lead Auditor Signature: _____

Cloud Service Provider Background

Overview of service offering:

Google Cloud Services include Google Cloud Platform and Google Workspace. Google Cloud Platform provides Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Customers can benefit from the performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model. Google Workspace products are composed of communication, productivity, collaboration and

security tools that can be accessed virtually from any location with internet connectivity. The products provide multi-user collaboration without requiring special hardware or software.
Service model: ☐ Virtual machine instances owned by the cloud service customer ☐ Network facilities ☑ **Compliance with applicable standards** Deployment model: ☐ Private cloud ☐ Community cloud ☐ Hybrid cloud ☑ **Public cloud** Tier: ☐ Level 1 ☐ Level 2 ☑ **Level 3**

No.	Criteria	Description	Remarks
Legal and Compliance			
1.	Right to audit	The cloud service customer has the right to audit: ☑ **Virtual machine instances owned by the cloud service customer** ☐ Network facilities ☐ Compliance with applicable standards ☐ Technical controls ☐ Policies and governance ☐ Data center facilities ☑ **Others <u>Right to audit is specific to customer contractual terms</u>** ☐ None Regulators recognised by Singapore law have the right to audit: ☐ Virtual machine instances owned by the cloud service customer ☐ Network facilities ☐ Compliance with applicable standards ☐ Technical controls	Our customers and regulators expect independent verification of security, privacy and compliance controls. Google undergoes several independent third party audits on a regular basis to provide this assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure, products, and operations. Google's third party audit approach is designed to be comprehensive in order to provide assurances of Google's level of information security with regard to confidentiality, integrity, and availability. Customers may use these third party audits to assess how Google's products can meet their security and privacy compliance requirements. Clauses 15.2.2(b), and 15.2.3(b) are not applicable as third-party scanning tools

		☐ Policies and governance ☐ Data center facilities ☐ Others _____ ☑ **None** Audit / assessment reports that can be made available on request: ☑ **Penetration test** ☐ Threat and vulnerability risk assessment ☐ Vulnerability scan ☑ **Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)**	sometimes are unable to take all mitigating factors of Google's environment into consideration when reporting vulnerability severity. Google's internal Vulnerability Management relies on severity ratings of findings that scanners report rather than the CVSS values. As a result, Google defines vulnerability prioritization according to a scale from P0-P4, where for example immediate attention is required for P0. Google will allow customers or an independent auditor appointed by the Customer to conduct audits to verify Google's compliance with its obligations under certain business terms set forth by Google in our Data Protection Agreement (section 7.5.2, and 7.5.3).
2.	Compliance	The following guidelines / standards / regulations are adhered to: ☐ Singapore Personal Data Protection Act ☑ **ISO / IEC 27001** ☑ **ISO 9000** ☐ ISO / IEC 20000 ☑ **CSA Open Certification Framework** ☑ **PCI-DSS** ☐ Others _____	Google is committed to protecting our cloud customers' data. We undergo several independent third-party audits on a periodic basis. For the complete and updated list, please visit https://cloud.google.com/security/compliance Google has provided documentation describing control environment in order to enable customers to evaluate the suitability of Google Cloud within the context of Singapore PDPA: https://services.google.com/fh/files/misc/singapore_personal_data_protection_act_whitepaper.pdf Google performs periodic evaluations of Cloud Service delivery and performs

			background checks on new hires, where legally permissible. As such, we believe we have addressed the risk for which Clause 7.2.4 is intended. Under Clause 8.2 Google performs an Enterprise-wide Risk Assessment for each Product Area twice per year. In addition, Google's Office of Compliance & Integrity team, Cloud Compliance & Certifications team, Internal Audit, and Security Teams coordinate the continual improvement and monitoring of the ISMS through the use of information security policies, information security objectives, audit results, analysis of continuous monitoring events, corrective and preventive actions, and management review.
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud service customer except for: _____ The cloud service customer retains the ownership on the derived data or attributes of cloud usage except for the following: ☑ **Advertising or marketing** ☑ **Statistics analysis on usage** ☑ **Others <u>Product Development</u>**	Google does not use customer content for marketing or advertising purposes. Google Cloud may advertise directly to Google Cloud customers to market additional services which may be of interest to those customers.
4.	Data retention	Data deleted by the cloud service customer is retained as follows: ☑ **Minimum data retention period is: <u>30 days (GCP); 20 days (Google Workspace)</u>** ☑ **Maximum data retention period is: <u>180 days</u>** ☐ Deleted immediately Log data is retained for a period of: ☑ **Minimum data retention period as follows: <u>30 to 400 days (GCP); 30 days to 15 months (Google Workspace)</u>**	Please refer to https://cloud.google.com/terms/data-processing-addendum section 6 https://cloud.google.com/security/deletion/#deletion_timeline https://support.google.com/a/answer/33314?hl=en https://cloud.google.com/logging/quotas#logs_retention_periods

		☑ **Maximum data retention period is: <u>30 to 400 days (GCP); 30 days to 15 months (Google Workspace)</u>** ☐ Not retained Cloud service customer data is retained for a period of: ☐ Minimum data retention period is: _____ ☐ Maximum data retention period is: _____ ☐ Not retained The following types of data are available for download by the cloud service customer: ☑ Log data ☑ **Others <u>Any user data</u>**	https://support.google.com/a/answer/7061566 Clause 13.5.3(b) - Google ensures that Logs datasets are collected, stored, managed, and accessed in adherence to Google's internal and external privacy policies through the use of dedicated logs infrastructure. Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate Customers are responsible for logging and monitoring changes in a cloud user's administrators account in accordance with clause 23.9. For Clause 23.9.4, Google has provided the Cloud Identity Terms of Service that states the customer agrees that Google's responsibilities do not extend to the internal management or administration of the services for customers and that Google is merely a data processor. https://cloud.google.com/terms/identity/na_terms
5.	Data sovereignty	The primary data locations are: ☐ Singapore ☐ Asia Pacific _____ ☐ Europe _____ ☐ United States ☑ **Others** **https://cloud.google.com/about/locations/** **https://www.google.com/about/datacenters/locations/** The backup data locations are: ☐ Singapore	**GCP** For certain Google Cloud Platform services, customers may select where their data will be stored (the "Data Location Selection"), and Google will store the data in accordance with the Service Specific Terms. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location Selection is not made by Customer in respect of any Customer Data), Google may store and process the relevant Customer Data anywhere Google or its Subprocessors

		☐ Asia Pacific _____ ☐ Europe _____ ☐ United States ☑ **Others <u>See above</u>** No. of countries in which data centers are operated: _____ The cloud service customer's data stored in the cloud environment will never leave the locations specified in item 5: ☐ Yes ☐ Yes, except as required by law ☐ Yes, except as noted: _____ ☑ **No** Cloud service customer's consent is required prior to transferring data to a location not specified in item 5 or a third party: ☐ Yes ☑ **Yes, except as required by law** ☐ Yes, except as noted: _____ ☐ No *Note: Cloud service customers are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, cloud service customers should understand the risks associated with relevant laws that may allow for law enforcement or other government access to data in-transit or storage with Cloud Service Providers.*	maintains facilities. Google stores data in a multi-tenant environment on Google-owned servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. https://cloud.google.com/about/locations Per requirement 18.5.2(d) "Visitors' log is periodically reviewed": Google has established formal access procedures allowing physical access to the data centers. There are documented procedures for issuing badges to staff and/or visitors and the owner of each badge is tracked and documented. All entrants to the data center, whether Google employees, visitors, or contractors, must identify themselves and show proof of identity to security operations. Valid proof of identity consists of (1) a photo ID issued by Google or (2) a governmental entity. Authorized Google Data Center Approvers must approve all visitors in advance for the specific data center and internal areas they wish to visit. After the individual's access authorization is verified, the visit is logged, and access is granted for the specified dates and times. These logs are retained by Google security for review as needed. Visitors are provided a temporary badge and must be escorted by an authorized Google employee to access areas beyond the lobby. When the visitors leave the data center, they must return the visitor badge.

			Google Workspace Per section 10 of the Cloud Data Processing Addendum, Customer Data may be processed in any country where Google or its Subprocessors maintain facilities, subject to Google's data location commitments under the Service Specific Terms and data transfer commitments. The locations of Google Workspace data centers are described at https://www.google.com/about/datacenters/locations/ Unless specifically disclosed for a given product, Google Cloud does not host data at any third party data centers where Google does not own and manage the physical security boundary and control therefore clauses 9.3.4(a) and 9.5.4(d) are not applicable to the Google environment. **Google Cloud NetApp Volumes (GCNV)** Google Cloud offers the GCNV product through GCP, which relies on a subprocessor to provide certain aspects of the service. The subprocessor engages third party data center services for hosting. These third party data centers are excluded from the scope of this audit.
6.	Non disclosure	☑ **Non-disclosure agreement template can be provided by Cloud Service Provider** ☑ **Cloud Service Provider may use customer's NDA (pending legal review)**	Google ensures that a non-disclosure agreement is in place before sharing any confidential information with any customer. Google will also work with the customer if they request to use their NDA template.
Provider Performance			
7.	Availability	The committed network uptime is: ☐ _____%	https://cloud.google.com/terms/sla/

		☐ Varies according to price plan The committed system uptime is: ☐ _____% ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☐ None	https://workspace.google.com/intl/en/terms/sla.html
8.	3rd party dependency	Highlight areas of critical dependency for service delivery: None/Not applicable	**Edge/Points of Presence (PoPs) locations:** Edge/PoP locations are not critical elements or represent any critical dependency of Google service offerings, but are used for reducing network latency. Google Cloud services might utilize compute, storage, and other cloud services within non-Google Edge/PoPs location. Presently Google is not validating the design or operating effectiveness of physical security at these Edge/PoP facilities. Google has implemented appropriate compensating controls to mitigate the above risk: 1. The PoP vendors do not have logical access to the Google services, and they are only responsible for providing space and power. 2. Access management controls are leveraged to define ACLs (in Ganpati) that prevent unauthorized access to customer data. 3. Furthermore Google has implemented robust encryption controls for data at rest and in transit between two production environments. 4. Robust logging and monitoring

			controls have been implemented for auditing access to data. 5. Private key material for termination of SSL is not stored on the machines in non-Google edge POPs. Based on the above assertions of no critical dependency on Edge/PoP locations and compensating controls in place, Edge/Pop locations will be out of scope for this audit. **Google Cloud NetApp Volumes (GCNV)** Google Cloud offers the GCNV product through GCP, which relies on a subprocessor to provide certain aspects of the service. The subprocessor engages third party data center services for hosting. These third party data centers are excluded from the scope of this audit.
9.	BCP / DR	☐ Disaster recovery protection ☐ Backup and restore service ☐ Cloud service customer selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☑ **RPO <u>SRO Program</u>** ☑ **RTO <u>SRO Program</u>** ☐ Others, please specify: _____	Google has an SRO (service recovery objective) program for zonal and regional failure events. These RPO/RTO commitments are provided to customers in order to provide proof of disaster preparedness by covering cloud architecture, risk, and business continuity planning. Google replicates data over multiple locations to help protect against accidental destruction or loss. GCP customers may schedule their own backups using provided services, such as Cloud archival or Cold Storage. Per requirement 21.2.2(e): "The Cloud Service Provider shall develop, maintain and communicate a BCP framework for the required cloud services. The framework includes, but is not limited to, the following

			requirements: e) Determination of maximum tolerable period of disruption." Google does not perform traditional contingency planning and therefore does not conduct a traditional information system-wide business impact analysis to determine maximum tolerable downtime or data loss. Instead Google has established an internal service level agreement framework between infrastructure teams and internal customers that allow our services to achieve stated service levels within our agreements. SLAs for each service are published at: https://cloud.google.com/terms/sla
10.	Liability	The following terms are available for the cloud service customers on failure of the provider to meet the service commitment: ☐ Network failure Liability: _____ _____ ☐ Infrastructure failure Liability: _____ _____ ☐ Virtual machine instance failure Liability: _____ _____ ☐ Migrations Liability: _____ _____ ☐ Unscheduled downtime Liability: _____ _____ ☐ Database failure Liability:	Google shall use all reasonable commercial efforts to ensure that all the GCP services are operated and available to customers based on the service level agreements described below. In the event Customer experiences any of the service performance issues defined below due to Google's failure to provide Services, Customer will be eligible to receive the Service Credits described below. https://cloud.google.com/terms/sla/ During the Term of the applicable Google Workspace Agreement, the Google Workspace Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the "Google Workspace SLA"). If Google does not meet the Google Workspace SLA, and if Customer meets its obligations under this Google Workspace SLA, Customer will be eligible to receive the Service Credits described below. This Google Workspace SLA states Customer's sole and exclusive remedy for any failure by

		_____ _____ ☐ Monitoring failure Liability: _____ _____	Google to meet the Google Workspace SLA. https://workspace.google.com/intl/en/terms/sla.html
11.	Shared responsibility	☑ **Communication of shared roles & responsibilities for which CSC needs to implement and manage for use of this cloud service** **URL (or attach file): (see remarks)**	https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate https://services.google.com/fh/files/misc/gcp_pci_dss_v4_responsibility_matrix.pdf
Service Support			
12.	Change management	The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services: ☑ **Communication plan and procedures for proactive notification** ☑ **Assistance in migration to new services when legacy solutions are discontinued** ☐ Ability to remain on old versions for a defined time period ☐ Ability to choose timing of impact	https://cloud.google.com/terms/tssg/ https://workspace.google.com/terms/premier_terms/
13.	Self-service provisioning and management portal	Provide self-service provisioning and management portal for cloud service customers to manage cloud services: ☑ **Yes** ☐ No If yes, describe the functions of the self-service provisioning and management portal provided: ☑ **Allow role-based access control (RBAC)** ☑ **Manage resource pools (e.g. VMs, storage, and network) and service templates**	Google's self service platform provides users the ability to administer users and manage their Google services. Additionally, Cloud users are able to manage resource pools through the consoles and track usage statistics.

		☑ **Track and manage the lifecycle of each service** ☑ **Track consumption of services** ☐ Health monitoring ☐ Others: _____	
14.	Incident and problem management	Delivery mode of support: ☑ **Access via email** ☑ **Access via portal** ☑ **Access via phone support** ☑ **Direct access to support engineers** Availability of support: ☑ **24 x 7** ☐ During office hours support, please specify the hours of operations: _____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: _____ Notification time of cloud service outage incident: _____ Communication channel used for notification of cloud service outage incident: _____ The following are available to cloud service customers upon request: ☐ Permanent access to audit records of customer instances ☑ **Incident management assistance** Incident response time: _____ Mean time to repair on detection of faults: __	https://cloud.google.com/support/?options=premium-support#options https://workspace.google.com/support
15.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☑ **Pay per usage (see remarks) (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per cloud service customer per hour/day/month/year for SaaS)** ☐ Fixed pricing_____(up to	Information about Google Cloud & G Suite Pricing may be found at: https://cloud.google.com/pricing/ https://workspace.google.com/pricing.html

		yearly/monthly/daily) ☐ Other pricing model _____ ☐ Not disclosed ☐ Available billing history: _____ Months	
16.	Data portability	Importable VM formats: _____ Downloadable formats: JSON/XML/other open formats (to specify) _____ Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: _____ Policy/guide available _____ API: ☐ Common _____ ☐ Customised _____ Upon service termination or prolonged outage, data is available through: ☐ Physical media ☑ **Standard methods as described above** ☐ Other methods _____	https://cloud.google.com/migrate/ https://cloud.google.com/migrate/virtual-machines/docs/5.0/discover/migrating-vms-migrate-for-compute-engine-getting-started https://support.google.com/accounts/answer/3024190?hl=en https://cloud.google.com/security/gdpr/ https://takeout.google.com/?pli=1 https://support.google.com/a/answer/100458?hl=en https://cloud.google.com/security/compliance/swipo-codes
17.	Interoperability	Use of industry standards and availability of APIs to support interoperability: ☐ Transport supported (e.g. REST based HTTPS/MQTT) _____ ☑ **Format supported (e.g. JSON/XML) <u>XML</u>** ☐ APIs supported _____ ☐ Other methods _____ **Guide available <u>(see remarks)</u>**	https://cloud.google.com/storage/docs/interoperability
18.	Access	Type of access to the service is through: ☑ **Public access** ☑ **Private access (e.g. VPN, dedicated link)**	In addition to the methods to the left, Google also offers Interconnect to its GCP customers. https://cloud.google.com/interconnect

		☑ **IPv6 access is supported** ☑ **Other access methods <u>Google Interconnect</u>** Public access speed (shared bandwidth) in Mbps: _____	Google Cloud Interconnect allows Google Cloud Platform customers to connect to Google via enterprise-grade connections with higher availability and/or lower latency than their existing Internet connections. Connections are offered by Cloud Interconnect service provider partners, and may offer higher SLAs than standard Internet connections. Google also supports direct connections to its network through direct peering. Customers who cannot meet Google at its peering locations, or do not meet peering requirements, may benefit from Cloud Interconnect. https://cloud.google.com/interconnect/
19.	User management	☑ **Identity management** ☑ **Role based access control** ☑ **Federated access model** ☑ **Integration with Identity management solutions** ☐ Others _____	Google offers Cloud Identity & Access management that allows administrators to authorize who can take action on specific resources, giving them full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across customer's organization, with built-in auditing to ease compliance processes. https://cloud.google.com/security/products/iam https://cloud.google.com/identity/ Below MTCS clauses are not applicable: Clause 22.13 is not applicable as third party admins do not have access. Clause 22.14 is not applicable as service and application accounts are not used https://cloud.google.com/terms/data-processing-terms

			Google has adopted NIST guidance (SP 800-63c) and, as such, does not enforce password history and rotation requirements as defined in Clause 22. Google's password policies provide “equivalent or better security” than the requirements established in Clause 22. Google has provided the ability to integrate customer's SSO via SAML, which allows them to configure their password settings to meet MTCS standards. As such, we consider this an alternative implementation to meet the requirements in Clause 23. Clauses 23.3, 23.5.2(a) and (b), 23.8.2(b) are not applicable as user access security is a shared responsibility between Google & Customer. Under Clause 22.5 and 23.5 Google has implemented the lockout control where a user is allowed 30 login attempts within a 3 hour period. If that number of attempts is met, then a user is unable to login for a 3 hour period. Additionally, customers are responsible for removing custom applications accounts, user IDs, passwords, test data and in accordance with clauses 16.2.2(b) and (c). Google employs robust, proprietary services and mechanisms to encrypt Google Workspace user data, as such, we believe we are addressing the risk for which clause 24.7.4(a) is intended. Clause 17.3.2(a) is not applicable as GCP customers can manage the keys themselves

			by using Cloud KMS or bring their own keys to Google Cloud. For the GCNV product, encryption of data-in-transit is a shared responsibility between Google and the customer. Clauses 17.4.3(g) and (h), and 17.4.4 are the responsibility of GCP customers to the extent that they utilize our Customer Managed Key capability, thereby using Hardware Security Module (HSM). Clauses 17.4.3(g) and (h), and 17.4.4 are not applicable for Google Workspace as Google does not use HSMs for internal key management systems (KMS). Cloud Customer Managed Encryption Keys https://cloud.google.com/storage/docs/encryption/customer-managed-keys Cloud HSM https://cloud.google.com/security/products/security-key-management Google Workspace Key Management https://support.google.com/a/answer/10741897 https://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf Please refer to Google's Encryption at Rest in Google Cloud Platform security whitepaper for additional information. https://cloud.google.com/security/encryption-at-rest/default-encryption/
20.	Lifecycle	The cloud service customer may select the following for service upgrades and changes: ☑ **Automatic provisioning** ☐ Cloud service customer customisable provisioning	https://cloud.google.com/identity/solutions/automate-user-provisioning

Security Configurations			
21.	Security configuration enforcement checks	Security configuration enforcement checks are performed: ☐ Manually ☑ **Using automated tools** How often are enforcement checks being performed to ensure all security configurations are applied? _____	https://cloud.google.com/docs/security/overview/whitepaper#vulnerability_management https://workspace.google.com/learn-more/security/security-whitepaper/page-3.html#vulnerability-management https://cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings
22.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☑ **Virtual instance grouping** ☑ **Cloud service customer definable security domains** ☑ **Cloud service customer customisable firewall** ☑ **Cloud service customer definable access policies**	Per requirement 14.3.4(b): "Any user-provided code is sandboxed or isolated to ensure the underlying platform and other tenants are not affected by the same." Google applies the Principle of Shift Left to our software development life cycle by doing as much testing as possible, as early as possible. The four different phases in the qualification cycle (pre-submit, post-submit, release qualification, and deployment) increases confidence by mitigating security-risk concerns to ensure that user-provided code does not affect the underlying platform. https://cloud.google.com/solutions/shifting-left-on-security Clauset 24.4.2(l) is not applicable as Google does not follow the concept of traditional hypervisors for products deployed in Google's prod/Borg infrastructure.
23.	Hybrid cloud provision	Ability to monitor, track, apply and enforce CSC's security & privacy policies on its cloud workloads: ☑ **Data protection and encryption key mgmt. enforcement geolocation-based / resource pools and secure migration of**	Option 1-2 References: https://cloud.google.com/storage/docs/encryption/customer-managed-keys https://cloud.google.com/docs/geography-and-regions#geographic_management_of_data

		cloud workloads ☑ **Key mgmt. and keystore controlled by CSC** ☐ Persistent data flow segmentation before and after geolocation based/resource pools secure migration ☑ **Compliance enforcement for regulated workloads between on premises private and hybrid/public cloud** ☐ Others _____	https://cloud.google.com/architecture/migrations Option 4 References: https://cloud.google.com/architecture/hybrid-and-multi-cloud-network-topologies General Hybrid Cloud Documentation https://cloud.google.com/architecture/hybrid-and-multi-cloud-patterns-and-practices https://cloud.google.com/architecture/hybrid-and-multi-cloud-patterns-and-practices#migration_and_modernization https://cloud.google.com/architecture/hybrid-and-multi-cloud-architecture-patterns
Service Elasticity			
24.	Capacity elasticity	The following capacity elasticity options are available: ☑ **Programmatic interface to scale up or down** ☐ Mean time to start and end new virtual instances _____ ☑ **Alerts to be sent for unusual high usage** ☐ Minimum performance during peak periods _____ ☐ Minimum duration to scale up computing resources _____ ☑ **Minimum additional capacity guaranteed per account <u>2 TB</u> (number of cores and GB memory)**	Google's Instance groups offer GCP customers managed groups that can automatically scale the number of instances in the group, work with load balancing services to distribute traffic to all of the instances in the group and automatically recreate the instance in the event of an incident. In addition to the automatic load balancing, Google also offers Health Checks that checks the health of the instance and the server. https://cloud.google.com/compute/docs/instance-groups/ https://cloud.google.com/compute/docs/load-balancing/health-checks

25.	Network resiliency and elasticity	The following network resiliency and elasticity options are available: ☑ **Redundant Internet connectivity links** ☑ **Redundant Internal connectivity** ☐ Selectable bandwidth up to _____ Mbps ☐ Maximum usable IPs _____ ☐ Load balancing ports _____ ☐ Load balancing protocols _____ ☑ **Anti-DDOS protection systems or services** ☐ Defence-in-depth mechanisms, please specify: _____ ☐ Network traffic isolation, please specify: _____ ☐ Shared or dedicated bandwidth, please specify: _____ ☐ QoS traffic control services ☑ **Alerts to be sent for unusual high usage** ☐ Minimum performance during peak periods _____ ☐ Minimum period to scale up network throughput _____	https://cloud.google.com/docs/security/overview/whitepaper#security_benefits_of_our_global_network https://cloud.google.com/docs/security/infrastructure/design#secure-internet
26.	Storage redundancy and elasticity	The following storage redundancy and elasticity options are available: ☑ **Redundant storage connectivity links within each data center** ☑ **Redundant storage connectivity links between data centers belonging to the same cloud** ☐ Storage traffic isolation, please specify: _____ ☐ Shared or dedicated storage network bandwidth, please specify: _____ ☐ Quality of service storage traffic control services ☐ Maximum storage capacity for entire cloud, please specify: _____	Google offers various storage options to customers based on their need: https://cloud.google.com/storage/ https://support.google.com/googlecloud/answer/6056635?hl=en&ref_topic=6055719 Clause 24.6 is not applicable since within Google the concept of SAN is not applicable. Google offers multiple storage solutions through a redundant architecture across geographically distributed DCs. All the machines within a DC are treated at the same "trust" level and hence have the same security configuration applicable.

		☐ Maximum storage capacity for single cloud service customer, please specify: _____ ☐ Maximum expandable storage, please specify: _____ ☑ **Alerts to be sent for unusual high usage** ☐ Minimum storage I / O performance during peak periods _____ ☐ Minimum period to scale up storage I / O throughput _____	