Certificate

Certificate number: 2018-014

Certified by EY CertifyPoint since: July 10, 2018

Based on certification examination in conformity with defined requirements in Multi-Tier Cloud Security – SS 584:2015 as defined and implemented by

Google Asia Pacific Pte Ltd*

located in 70 Pasir Panjang Road, Mapletree Business City, Singapore 117371 is compliant with the Level 3 requirements as stated in the standard:

Multi-Tier Cloud Security (MTCS) – SS 584:2015

Issue date of certificate: August 28, 2018

Expiration date of certificate: July 9, 2021

EY CertifyPoint will, according to the certification agreement dated December 17, 2015, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

The certification is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for multi-tier cloud security.

J. Sehgal | Director, EY CertifyPoint

Google Asia Pacific Pte Ltd

Scope for certificate 2018-014

The scope refers to level 3 of Multi-Tier Cloud Security System of Google Asia Pacific Pte Ltd located in 70 Pasir Panjang Road, Mapletree Business City, Singapore 117371 supporting the provision of Google Cloud using Infrastructure-as-a-service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) model.

Google Cloud Platform

- App Engine
- App Engine Flexible Environment
- BigQuery
- BigQuery Data Transfer Service
- Cloud Armor
- Cloud Bigtable
- Cloud Billing API
- Cloud CDN
- Cloud Console
- Cloud Console Mobile App
- Cloud Dataflow
- Cloud Datalab
- Cloud Dataproc
- Cloud Datastore
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud Firestore
- Cloud Functions
- Cloud Healthcare API
- Cloud Identity & Access Management
- Cloud Identity-Aware Proxy
- Cloud Interconnect
- Cloud IoT Core
- Cloud Jobs Discovery
- Cloud Key Management Service
- Cloud Launcher
- Cloud Load Balancing
- Cloud Machine Learning Engine
- Cloud Natural Language API
- Cloud Pub/Sub
- Cloud Resource Manager
- Cloud Router
- Cloud SDK
- Cloud Security Scanner
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speech-to-Text
- Cloud SQL
- Cloud Storage
- Cloud Storage Transfer Service
- Cloud Translation API
- Cloud Video Intelligence API
- Cloud Vision API
- Cloud VPN
- Compute Engine
- Container Builder
- Container Registry
- Data Loss Prevention API
- Dialogflow Enterprise Edition
- Genomics
- Google Service Control
- Kubernetes Engine
- Orbitera
- Persistent Disk
- Service Consumer Management API
- Service Management API
- Stackdriver Debugger
- Stackdriver Error Reporting
- Stackdriver Logging
- Stackdriver Profiler
- Stackdriver Trace
- Transfer Appliance
- Virtual Private Cloud (VPC)

This scope (edition: July 10, 2018) is only valid in connection with certificate 2018-014.

Digital version

Google Asia Pacific Pte Ltd

Scope for certificate 2018-014

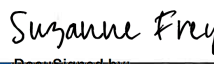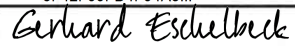The following locations are in scope:

Data Centers:

- Atlanta, Georgia, United States of America (ATL/IDI)
- Atlanta, Georgia, United States of America (ATL/MET)
- Changhua, Taiwan (TPE/CHG)
- Council Bluffs, Iowa, United States of America (CBF/CBF)
- Council Bluffs (Southland), Iowa, United States of America (CBF/SLN)
- The Dalles, Oregon, United States of America (DLS/DLS)
- Dublin, Ireland (DUB/PPK)
- Eemshaven, Groningen, Netherlands (GRQ/EEM)
- Ghlin, Hainaut, Belgium (BRU/GBL)
- Hamina, Finland (LPP/LPP)
- Lenoir, North Carolina, United States of America (CHS/MNK)
- Moncks Corner, South Carolina, United States of America (CHS/MNK)
- Pryor Creek, Oklahoma, United States of America (TUL/PRY)
- Quilicura, Santiago, Chile (SCL/QCA)
- Wenya, Singapore (SIN/WEN)
- Koto-ku, Tokyo, Japan (KOT)
- Ashburn, Virginia, United States of America (IAD)
- London, United Kingdom (SGH)
- Frankfurt, Hesse, Germany (ROD)
- Sydney, NSW, Australia (MQP)
- Montreal, Quebec, Canada (YUL)
- Sao Paulo, Brazil (OCO)
- Mumbai, India (MRL)

Digital version

Annex A
(normative)

Cloud service provider disclosure

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, the public Cloud Service Provider shall indicate accordingly with remarks.

Cloud Service Provider Contact Information

Company name: Google Asia Pacific Pte Ltd.
Primary address: 70 Pasir Panjang Road #03-71,
Mapletree Business City II
Singapore, 117371

Web address: https://cloud.google.com
Contact name: _____
Contact number: _____
MTCS certificate number: _____

Company stamp: _____ Signature of company representative: _____

DocuSigned by:

Suzanne Frey
3F42F99FD4F94A3...

Gerhard Eschelbeck
B0A6790040864C0...

Certification Body Contact Information

Company name: EY CertifyPoint
Web address: http://www.ey.com/gl/en/services/specialty-services/certifypoint
Contact name: Jatin Sehgal
Contact email: jatin.sehgal@nl.ey.com

Company stamp: _____ Signature of lead auditor: _____

Cloud Service Provider Background

Overview of service offering:

Google Cloud lets you focus on what's next for your business. Google Cloud frees you from the overhead of managing infrastructure, provisioning servers and configuring networks. To let innovators innovate and let coders, well, just code. From Gmail to Docs, Drive, and Calendar, collaborate with Google Cloud anytime, anywhere across your computer, phone, and tablet.

Service model:
☐ Virtual machine instances owned by the user
☐ 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 user has the right to audit: ☐ Virtual machine instances owned by the user ☐ Network facilities ☐ Compliance with applicable standards ☐ Technical controls ☐ Policies and governance ☐ Data centre 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 user ☐ Network facilities ☐ Compliance with applicable standards ☐ Technical controls ☐ Policies and governance ☐ Data centre 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)	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 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 compliance and data-processing needs. Google will allow customers or an independent auditor appointed by the

			Customer to conduct audits to verify Google's compliance with its obligations under our terms, as indicated in our Data Protection Agreement (section 7.5.2).
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 your organization's data. We undergo several independent third-party audits on a regular basis. For the complete and updated list, please visit https://cloud.google.com/security/compliance Google reviews the Information Security Policy annually and has processes in place to ensure that Information Security Policies and supporting guidance are current and aligned with the needs of the organization. As such, we believe we are addressing the risk for which clause 6.5.3a is intended. Google performs periodic evaluations of Cloud Service delivery and performs background checks on new hires, where background checks are allowed. As such, we believe we have addressed the risk for which clause 7.1.4a is intended.
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud user except	Google does not use user data for any

		for:_____ The cloud User retains the ownership on the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing ☑ Statistics analysis on usage ☐ Others_____	marketing or advertising purposes.
4.	Data retention	Data deleted by the user is retained as follows: ☑ Minimum data retention period is: <u>30 days</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>_____</u> ☐ Maximum data retention period is: <u>_____</u> ☐ Not retained User data is retained for a period of: ☐ Minimum data retention period is: <u>_____</u> ☐ Maximum data retention period is: <u>_____</u> ☐ Not retained The following types of data are available for download by the cloud user: ☑ Log data ☑ Other <u>any user data</u>	Please refer to https://cloud.google.com/terms/data-processingterms#7-data-correctionblocking-exporting-anddeletion for more details https://gsuite.google.com/terms/dpa_terms.html Log data is retained for one year.
5.	Data sovereignty	The primary data locations are: ☐ Singapore ☐ Asia Pacific_____ ☐ Europe_____ ☐ United States ☑ Other: https://cloud.google.com/about/locations/#regions-tab https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers The backup data locations are: ☐ Singapore ☐ Asia Pacific_____ ☐ Europe_____ ☐ United States ☑ Other <u>see above</u>	**GCP** For Google Cloud Platform services, customers may select where their data will be stored (the "Data Location Selection"), and Google will store it there in accordance with the Service Specific Terms. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location

| | | No. of countries in which data centres are operated: _____

The user'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

User'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 users are responsible for determining the impact of
data protection and data sovereignty laws on the locations where
data is stored. In addition, users 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. | 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 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/#regions-tab

G Suite

Per section 1.1 of the G Suite TOS, G Suite, as part of providing the services may transfer, store, and process customer data in countries where Google maintains facilities. To review our current list of datacenter locations where G Suite data is located, please see: https://www.google.com/about/datacenters/inside/locations/index.html |
| 6. | Non-disclosure | ☑ Non-disclosure agreement template can be provided by Cloud Service Provider

☑ Cloud Service Provider may use customer's | Google ensures that a non-disclosure agreement is in |

		NDA (pending legal review)	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: ☐ _____ % ☐ 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://cloud.google.com/terms/sla/ https://gsuite.google.com/intl/en/terms/sla.html
8.	BCP / DR	☑ Disaster recovery protection ☑ Backup and restore service ☐ User selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☐ RPO_____ ☐ RTO_____ ☐ Others, please specify: _____ _____	Google replicates data over multiple systems to help protect against accidental destruction or loss. Refer to SLAs https://cloud.google.com/terms/sla/ https://gsuite.google.com/intl/en/terms/sla.html
9.	Liability	The following terms are available for the users on failure of the provider to meet the service commitment: ☐ Network failure Liability:_____ ☐ Infrastructure failure	Google shall use all reasonable commercial efforts to ensure that all the GCP services are operated and available to customers 99.5% or more of the time in any

| | | | Liability:_____ | calendar month. 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 G Suite Agreement, the G Suite Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the ""G Suite SLA""). If Google does not meet the G Suite SLA, and if Customer meets its obligations under this G Suite SLA, Customer will be eligible to receive the Service Credits described below. This G Suite SLA states Customer's sole and exclusive remedy for any failure by Google to meet the G Suite SLA.

https://gsuite.google.co |
| --- | --- | --- | --- | --- |
| | | | ☐ Virtual machine instance failure | |
| | | | Liability:_____ | |
| | | | ☐ Migrations | |
| | | | Liability:_____ | |
| | | | ☐ Unscheduled downtime | |
| | | | Liability:_____ | |
| | | | ☐ Database failure | |
| | | | Liability:_____ | |
| | | | ☐ Monitoring failure | |
| | | | Liability:_____ | |

			m/intl/en/terms/sla.html
Service Support			
10.	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://gsuite.google.com/intl/en/terms/standard_terms.html https://gsuite.google.com/intl/en_in/terms/2013/1/premier_terms.html
11.	Self-service provisioning And management portal	Provide self-service provisioning and management portal for users 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 ☑ Track and manage the lifecycle of each service ☑ Track consumption of services ☐ Others:_____	Google's self service platform provides users the ability to administer users of the services. Additionally, Cloud users are able to manage resource pools through the consoles and track usage statistics.
12.	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: _____	https://cloud.google.com/support/?options=premium-support#options https://gsuite.google.com/support/

		The following are available to users upon request: ☐ Permanent access to audit records of customer instances ☑ Incident management assistance Incident response time: _____ Mean time to repair on detection of faults: _____	
13.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☑ Pay per usage _____ (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS) ☐ Fixed pricing_____(up to yearly/monthly/daily) ☐ Other pricing model_____ ☐ Not disclosed ☐ Available billing history: _____Months	Information about Google Cloud & G Suite Pricing may be found at https://cloud.google.com/pricing/ https://gsuite.google.com/pricing.html
14.	Data portability	Importable VM formats: _____ Downloadable formats: _____ Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: _____ API: ☐ Common _____ ☐ Customised _____ Upon service termination, data is available through: ☐ Physical media ☑ Standard methods as described above ☑ Other methods _____	https://cloud.google.com/migrate/ https://cloud.google.com/solutions/best-practices-migrating-vm-to-compute-engine https://support.google.com/accounts/answer/3024190?hl=en https://cloud.google.com/security/gdpr/
15.	Access	Type of access to the service is through: ☑ Public access	In addition to the methods to the left, Google also offers

		☑ Private access (e.g. VPN, dedicated link) ☑ IPv6 access is supported ☑ Other access methods <u>Google Interconnect</u> Public access speed (shared bandwidth) in Mbps: _____	Interconnect to its GCP customers. https://cloud.google.com/interconnect/ 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/
16.	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 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/iam/ https://cloud.google.com/identity/ Below clauses are not applicable: Clause 22.12 is not applicable as third party admins do not have access Clause 22.13 is not applicable as service and application accounts are not used Clause 23.2 is not applicable as user access security is a shared responsibility between Google & Customer 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 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. Google employs robust, proprietary services and mechanisms to encrypt G Suite user data, as such, we believe we are addressing the risk for which clause 24.6.4a is intended.
17.	Lifecycle	The cloud user may select the following for service upgrades and changes: ☑ Automatic provisioning ☐ User customisable provisioning	https://cloud.google.com/ identity/solutions/automate-user-provisioning
Security Configurations			
18.	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/ terms/data-processing-terms#7-data-correction-blocking-exporting-and-deletion https://cloud.google.com/ terms/data-processing-terms#appendix-2-security-measures https://gsuite.google.com/ terms/dpa_terms.html
19.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☑ Virtual instance grouping ☑ User definable security domains	https://cloud.google.com/ terms/data-processing-terms

		☑ User customisable firewall ☑ User definable access policies	
Service Elasticity			
20.	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__2TB____(number of cores and GB memory)	Google's Instance groups offers its GCP customers the 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 recreates the instance in the event of an incident. In additional 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
21.	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: _____ ☐Defence-in-depth mechanisms, 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 _____	
22.	Storage redundancy and elasticity	The following storage redundancy and elasticity options are available: ☑ Redundant storage connectivity links within each data centre ☑ Redundant storage connectivity links between data centres 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: _____ ☐ Maximum storage capacity for single user, 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_____	Google offers various storage options to customers based on their needs (https://cloud.google.com/storage/) https://support.google.com/googlecloud/answer/6056635?hl=en&ref_topic=6055719 MTCS Standard, Clause 24.5 is not applicable