1 Cloud Management- Managed GCP - Core Services

In order for NTT to manage the Client's GCP environment, the following requirements must be met and are client responsibilities:

1.1 Supported Configurations

(a) GCP Project with Owner/Contributor role

(b) Allow Application registration for monitoring and consumption tooling, provided by NTT.

1.2 Core Services

The following are the GCP core services:

As Public Cloud technology evolves at such a rapid pace, it is not possible to maintain a fully up-to-date list of supported features and services, this Service Description may be updated from time to time in NTT's sole and absolute discretion.

The services listed below are supported as part of this service description. The exact scope of the solution being delivered to the Client and related charges are clearly stated in the Statement of Work (SOW) and anything not in specifically included as In Scope in the SOW is specifically excluded as out of scope.

Category	Managed Element	Supported Services
Governance	Cloud Base Service	. GCP Projects . Folders . Cloud Logging . Cloud Asset inventory . Cloud IAM
	Cloud Region	. Virtual Private Cloud (VPC) . Cloud Storage . Cloud DNS . Cloud VPN . TCP Load Balancers . Cloud Key Management System (Cloud KMS) . Cloud NAT
Networking	Cloud PaaS & SaaS Networking	. Cloud CDN . HTTP(s) Load balancer . SSL Proxy LB
	Direct Connectivity	. Cloud Interconnect . Partner Interconnect
Network Security	Cloud PaaS & SaaS Network Security	. Cloud Armor
Compute	Cloud IaaS - Scaling Group (Elastic)	. Compute Engine Managed instance groups (MIGs)
	Cloud IaaS - VM (Static)	. Compute Engine
Automation	Cloud VM Scheduling [per vm]	. Cloud Deployment Manager

Table 1 GCP Core Services

1.3 Governance

(a) Base Cloud Managed Services

(i) Overview

This element of the service covers the configuration, and management of the governance of Google Cloud Platform environments. Charges are based on the number of GCP Projects that the Client has regardless of the resources deployed are managed or unmanaged as specified in the SOW.

(ii) Supported Technologies

- GCP Projects
- Folders
- Cloud Logging
- Cloud Asset inventory
- Cloud IAM

GCP Projects	
Overview	a GCP project is a container for GCP. It is used to organize and manage resources, as well as to track billing and usage information.
Setup Activities	. Create or takeover GCP Projects . Link Client domains to Google Cloud . Create one service account
Service Request	. Manage / Change Project Quotas . Tag resources . Move resources across project . Change Service Limits
Available Monitoring	Vendors provided service limits, which at least includes CPU count and number of VM.

Table 2 GCP projects

Folders	
Overview	Folders are a way of organizing resources within a GCP project
Setup Activities	. Create or takeover GCP Folders . Link Client domains to Google Cloud
Service Request	. Move Projects into folders . Moving folders

Table 3 GCP projects

Cloud Logging	
Overview	Cloud Logging is used to store, search, and analyze data events generated by GCP services
Setup Activities	. Enable Cloud Logging API to the projects . Configure log sinks
Service Request	. Enable/Disable cloud logging API . Request add specific logs . Export logs data from GCP to other services (BigQuery, Cloud Storage or Pub/Sub)
Service Limitation	Application troubleshooting and/or analysis of logs is not included as part of this service and is out of scope.

Table 4 GCP projects

Cloud Asset inventory	
Overview	Cloud Asset Inventory provides inventory services based on a time series database
Setup Activities	. Enable Cloud Asset API in the projects . Setup IAM permissions . Configure Assets discovery . Configure the inventory Settings
Service Request	. Change inventory settings

Table 5 GCP projects

Cloud AIM	
Overview	Cloud AIM provides access control and visibility for centrally managing cloud resources.
Setup Activities	. Grant AIM roles . Audit Role assignment

Sensitivity Label: General

Service Request	. Assign or change RBAC roles to restrict permissions

Table 6 Cloud AIM

1.4 Cloud Region

(a) Overview

Charges are based on the number of regions where resources are deployed as specified in the SOW. The management of all of services described in this section are covered, regardless of the number of resources deployed within the region where Managed IaaS resources or other cloud management services are contracted.

(b) Supported Technologies

- Virtual Private Cloud (VPC)
- Cloud Storage
- Cloud DNS
- Cloud VPN
- TCP Load balancers
- Cloud Key Management System (Cloud KMS)
- Cloud NAT

Virtual Private Cloud VPC	
Overview	Virtual Private Cloud (VPC) provides networking functionality to Compute Engine virtual machine (VM) instances, Google Kubernetes Engine (GKE) containers, and the App Engine flexible environment.
Setup Activities	. Create the VPC . Set the IP address range . set/define subnets . Create firewall rules . Crate firewall policies
Service Request	. Change/Add firewall rules . Change/Add firewall polices . Adjust MTU of a VPC

Table 7 GCP VPC

Cloud Storage	
Overview	Cloud Storage allows world-wide storage and retrieval of data at any time subject to GCP terms and conditions.
Setup Activities	. Create Buckets . Enable Data encryption
Service Request	. Download/Upload objects . Change RBAC . Change Storage Class
Available Monitors	.GetBucketMetadataReceivedBytes_raw .GetBucketMetaDataRequestCount_raw .GetBucketMetadataSentBytes_raw .ObjectCount .TotalBytes .GetBucketMetadataReceivedBytes .GetBucketMetaDataRequestCount .GetBucketMetadataSentBytes
Service Limitation	

Table 8 Cloud Storage

Cloud DNS

Sensitivity Label: General

Overview	DNS serving from Google's worldwide network for register, manage, and serve domains.
Setup Activities	. Create a Managed Public Zone . Point IP Address to a Domain . Create forwarding/peering zones . Configure DNS server Policies
Service Request	. Change/modify Zones . Change/modify IP Addresses of the Domain . DNS Policies modification . Activate DNSSEC
Available Monitors	. ResponsesFORMERR . ResponsesNOERROR . ResponsesNOTIMP . ResponsesNXDOMAIN . ResponsesSERVFAIL . ResponsesUNKNOWN . TotalResponses
Service Limitation	

Table 9 Cloud DNS

Cloud VPN	
Overview	Cloud VPN securely connects a *peer network* to a Virtual Private Cloud (VPC) network through an IPsec VPN connection.
Setup Activities	. Create the VPN Gateway . Configure peer VPN Gateway . Configure Firewall Rules . Generate pre-shared key . Add VPN Tunnels
Service Request	. Modify /add firewall Rules . Add/Delete VPN Tunnels
Available Monitors	. ResponsesFORMERR . ResponsesNOERROR . ResponsesNOTIMP . ResponsesNXDOMAIN . ResponsesSERVFAIL . ResponsesUNKNOWN . TotalResponses . DroppedReceivedPacketsCount . DroppedSentPacketsCount . ReceivedBytesCount . ReceivedPacketsCount . SentBytesCount . SentPacketsCount . SuccessfulReceivedPacketsCount . SuccessfulSentPacketsCount . TunnelEstablished
Service Limitation	. Configuration of a VPN gateway/ router to connect to Cloud VPN is not covered in this service

Table 10 Cloud VPN

TCP Load Balancer	
Overview	This element covers different cloud service like: . TCP proxy load balancer . TCP /UPD network load balancer . TCP / UDP load balancer

Sensitivity Label: General

Setup Activities	. Create and instance group . Configure backend service . Configure a health check . Configure a firewall rule . Create a TCP proxy . Configure a global forwarding rules
Service Request	. Change backends service and health-checks . Change firewall rules . Scaling the load balancer

Table 11 Cloud Load Balancer - TCP/UDP LB

Cloud NAT	
Overview	Cloud NAT provides fully managed, software-defined network address translation support for Google Cloud
Setup Activities	. Setup NAT configuration for the Elements on management . Configure Cloud NAT rules . Configure Organization policy constraints
Service Request	. Change NAT of the cloud resources . Change quotes and limits . Report a logging information
Service Limitation	Cloud NAT management covered in this SD apply only to a Managed Elements (VMs, GKE, Cloud Run, Cloud Function and App Engine)

Table 12 Cloud NAT

Only the specific service requests are in scope, otherwise any service request is out of scope.

1.5 Managed Infrastructure Services (Networking)

(a) PaaS and SaaS Networking

(i) Overview

This element of the service covers PaaS and SaaS Networking services on GCP. Charges are based on the number of instances of each technology present in the environment as specified in the SOW.

(ii) Supported Technologies

- Cloud CDN
- HTTPs Cloud Load Balancing

Cloud CDN	
Overview	Cloud CDN (Content Delivery Network) uses Google's globally distributed edge points of presence to cache external HTTP(S) load balanced content close to the end users
Setup Activities	. Configure the backend service (Instance groups, Zonal Network endpoint group, or Buckets) . Setup the SSL certificate resources . Enable Cloud CDN . Setting up Cache mode . Enable dynamic compression
Service Request	. Change Cache mode . Change TTL setting and overrides

Table 13 Cloud CDN

Cloud Load Balancing (Internal HTTPs load balancer)	
Overview	is a proxy-based, regional Layer 7 load balancer that enables to run and scale services behind an internal IP address.
Setup Activities	. Set IAM policies for cloud load balancing . Set organization policy constraints for cloud Load Balancing

	. Setup SSL certificates and permissions . Configure firewall rule . Configure forwarding rule protocol . Configure backend . Set connection duration lifetime . Configure session affinity . Set advance futures Traffic Steering, Traffic Actions and traffic policies
Service Request	. Change Loadbalancing parameters. . Change Traffic Steering, Traffic Actions and traffic policies
Available Monitors	. BackendRequestCount_raw . BackendResponseBytesCount_raw . Http200RequestCount_raw . Http300RequestCount_raw . Http400RequestCount_raw . Http500RequestCount_raw . HttpRequestCountFromAmerica_raw . HttpRequestCountFromAsia_raw . HttpRequestCountFromEurope_raw . RequestBytesCount_raw . RequestCount_raw . ResponseBytesCount_raw
Service Limitation	

Table 14 Cloud Load Balancing

Only the specific service requests are in scope, otherwise any service request is out of scope.

(b) Cloud Direct Connectivity

(i) Overview

This element of the service covers the connections between GCP data centers and Client premises.

(ii) Supported Technologies

- Dedicated Interconnect
- Partner Interconnect

Cloud Interconnect - Dedicated	
Overview	Mange Dedicated Cloud Interconnect provided by GCP.
Setup Activities	. Set connection type and capacity . Create the cloud Router
Service Request	. Create VLAN attachments . Creation and management of routes . Changes to the contracted bandwidth (additional cost from GCP)
Available Monitors	. attachmentCapacity . bytesReceived . bytesReceivedAttachment . bytesSent . bytesSentAttachment . circuitRxPower . circuitTxPower . egressErrors . ingressErrors . interconnectCapacity . packetsDropped . packetsReceived . packetsReceivedUnicast . packetsSent . packetsSentUnicast
Service Limitation	. Procurement of Cloud Interconnect and all procurement and provisioning related activities are Client's responsibility.

Table 15 Cloud Interconnect

Sensitivity Label: General

Cloud Interconnect - Partner	
Overview	Partner Interconnect provides connectivity between the Client's on-premises network and GCP Virtual Private Cloud (VPC) network through a GCP supported service provider
Setup Activities	. Set connection type and capacity . Create the cloud router
Service Request	. Create VLAN attachments . Creation and management of routes . Changes to the contracted bandwidth (additional cost from GCP)
Available Monitors	. Bytes: Received and Sent . Network Capacity . Packets: Received, Sent
Service Limitation	. Procurement of Cloud Interconnect and all procurement and provisioning related activities are Client's responsibility. Selection of GCP service providers are controlled by GCP.

Table 16 Partner Interconnect

Only the specific service requests are in scope, otherwise any service request is out of scope.

1.6 Managed Infrastructure Services (Security)

(a) PaaS and SaaS Network Security

(i) Overview

This element of the service covers the PaaS and SaaS Network Security services. Charges are based on the number of instances present in the environment as specified in the SOW.

(ii) Supported Technologies

- Cloud Armor

Cloud Armor	
Overview	Cloud Armor is a network security service that provides some defense against DDoS and application attacks, and offers a set of WAF rules
Setup Activities	. Create security policy . Create set of rules . Deploy the security policy
Service Request	. Integrate Cloud armor with cloud logging . Change the security policies
Service Limitation	Client must provide all details of the rules and security policy in order to be implemented including all technical details.

Table 17 Cloud Armor

1.7 Managed Infrastructure Services (Compute)

(a) IaaS Scaling Group (Elastic)

(i) Overview

This element of the service covers the compute engine Managed instance groups (MIGs). Charges are based on the number of scaling groups, regardless of the number of VMs that may be running during a certain period of time.

(ii) Supported Technologies

- Compute Engine Managed instance groups (MIGs)

Compute Engine Managed Instance Groups (MIGs)	
Overview	A Managed Instance Group is a collection of virtual machine (VM) instances that can be managed as a single entity.
Setup Activities	. Create and instance template . Configure the MIG

Sensitivity Label: General

	. Set up health checks . Configure auto-Scaling
Service Request	. Change the auto-scaling policies
Service Limitation	Operating System Management is not included and must be contracted separately.

Table 18 Compute Engine Managed instance groups (MIGs)

(b) IaaS- VM (Static)

(i) Overview

This element of the service covers the static VMs. Charges are based on the number of virtual machines under management as specified in the SOW.

(ii) Supported Technologies

- Compute Engine

Compute Engine Managed instance groups (MIGs)	
Overview	delivers virtual machines running in Google's data centers.
Setup Activities	. Create compute engine instance . Configure network setting . Setup backups . Setup VM scheduling
Service Request	. Scale up or down . Start/restart, stop and delete vms . change scheduling
Available Monitoring	. CPU Usage: Time, Utilization) . Disk read (bytes, ops, throttled bytes, throttled ops, IOPS) . Disk Write (bytes, ops, throttled bytes, throttled ops, IOPS) . Firewall Dropped (bytes, packets, bps, Packet Rate) . Network (In, Out, packetsIn, PacketsOut) . Reserved Cores . Uptime
Service Limitation	Operating System Management is not included and must be contracted separately.

Table 19 Compute Engine Managed instance groups (MIGs)