1 Public Cloud Management- Managed AWS - Core Services

This service provides the configuration, monitoring and management of the core services in an AWS environment which are specified as In Scope in the SOW.

1.1 Supported Configurations

(a) Client account not linked to an NTT Master Payer Account

(b) Client account linked to an NTT - End Client Master Payer Account

(c) Client account linked to an NTT - Reseller Master Payer Account

In each scenario, the Client retains ownership of their AWS account.

1.2 Client Responsibilities

(a) A minimum of Business Level Support from AWS is required on all managed accounts.

1.3 AWS Access Management Prerequisites

In order for NTT to manage the Client's AWS environment, the following requirements must be met:

(a) AWS Account with root access; or

(b) AWS Account with IAM user with full administrative rights

1.4 Core Services

Managed AWS covers the following core services:

(a) Governance Management

(b) Managed IaaS Resources

(i) Managed Compute

(ii) Managed Storage

(iii) Managed Network

(iv) Security

(c) Managed Cloud Identity

The services listed below are fully supported as part of this Service Description. 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 description, therefore, serves as a baseline across common categories.

The exact scope of the solution being delivered to the Client and related charges are clearly stated in the Statement of Work (SOW).

Category	Managed Element	Supported Services
Governance	Base	. AWS Organizations . AWS Accounts . AWS CloudTrail . AWS Config
	Region	. Amazon VPCs . Amazon S3 . Amazon Glacier . Amazon Route 53 . VPN Gateways . AWS IAM . AWS KMS . AWS ACM . AWS Secrets Manager . AWS License Manager . CloudWatch . CloudHSM
Managed Infrastructure Services	PaaS and SaaS Networking	. Amazon CloudFront . Elastic Load Balancing . AWS Transit Gateway
	PaaS and SaaS Security	. AWS WAF
		. AWS Network Firewall

Category	Managed Element	Supported Services
		. AWS Firewall Manager
		. AWS Amazon Inspector
		. AWS Security Hub
		. AWS Guard Duty
	Direct Connectivity	. AWS Direct Connect
	Hardware Security Module (HSM) for public clouds	. AWS CloudHSM
Compute	IaaS - Scaling Group (Elastic)	. Amazon EC2 Auto Scaling
	IaaS - VM (Static)	. Amazon EC2
Storage	Cloud PaaS File Storage	. Amazon EFS . Amazon FSx for Windows File Server
Cloud Identity	Cloud Identity & domain	. AWS Directory Service . AWS Single Sign-on
	Cloud Hybrid Identity	. AWS Cognito
Data Protection	Cloud Backup	. AWS Backup

Table 1 AWS Core Services Summary

Governance

1.5 Base Cloud Managed Services

(a) Overview

This element of the service covers the base management configuration required for every Client. Charges are based on the number of organizations and accounts that are deployed as specified in the SOW. All services are covered and must be included in Charges, regardless of the number of resources deployed within the Client landscape.

(i) Supported Technologies

- AWS Organizations
- AWS Accounts
- AWS CloudTrail
- AWS Config

AWS Organizations	
Overview	An AWS Organization is a logical grouping of AWS Accounts belonging to the same Client
Setup Activities	. Create or takeover AWS Organization . Create Organizational Units (OU) hierarchy . Create and apply Service Control Policies (SCP) . Create new accounts
Service Request	. Apply Client provided SCP . Create additional OU . Create additional accounts
Service Limitation	. Design Organization strategy . Creation of additional customized SCPs

Table 2 AWS Organizations

AWS Account	
Overview	An AWS Account is a logical container used to provision resources in AWS
Setup Activities	. Create or takeover AWS Account . Associate the AWS Account to an existing AWS Organization
Service Request	. Open support cases to AWS . Manage service limits
Service Limitation	. Cost Advisory or Security Advisory

Table 3 AWS Account

AWS CloudTrail	
Overview	AWS CloudTrail enables auditing, security monitoring, and operational monitoring by logging your AWS account activity
Setup Activities	Enable AWS Config (CT doesn't work without it), apply standard monitoring protocols, link to external monitoring apps
Service Request	Create new monitoring protocol, enable third-party app access
Service Limitation	Develop custom automated serverless response (i.e. Cloudtrail > Step Functions > Lambda > IAM policy change

AWS Config	
Overview	AWS Config is a service to assess, audit, and evaluate the configurations of AWS resources.
Setup Activities	Enable, apply standard monitoring protocols, link to external monitoring apps
Service Request	Create new protocols, enable third-party app access
Service Limitation	Develop custom automated serverless response

(b) Cloud Region

(i) Overview

This element of the service covers the services that are deployed by Cloud Region. Charges are based on the number of Regions that are deployed as specified in the SOW. All services are covered and must be included in the Charges section of the SOW, regardless of the number of resources deployed within the Region.

(ii) Supported Technologies

- Amazon VPCs
- Amazon S3
- Amazon Glacier
- Amazon Route 53
- VPN Gateways
- AWS IAM
- AWS KMS
- AWS ACM
- AWS Secrets Manager
- AWS License Manager
- AWS CloudWatch
- AWS CloudHSM

Amazon VPC	
Overview	Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that Client has defined.
Setup Activities	. Create VPC . Create Subnets . Create Route tables . Create Internet Gateways . Create VPC Endpoints . Setup VPC Peerings . Setup AWS PrivateLink . Setup VPC Flow logs . Setup Network ACLs . Create NAT gateways . Setup internal DNS resolution . Setup prefix lists
Service Request	. Addition of CIDR block . Addition of subnets . Update route table rules . Enable or modify VPC Flow Logs . Modify Network ACLs . Create or modify VPC Endpoints . Create or modify AWS PrivateLinks . Manage setup prefix lists
Service Limitation	

Table 4 Amazon VPC

Amazon Simple Storage Service (S3)	
Overview	Object storage service
Setup Activities	. Create S3 buckets . Configure access policies to S3 buckets . Enable encryption on S3 buckets . Configure data lifecycle policies (expiration, move to Glacier, change Storage Tier, etc.) . Enable access logging
Service Request	. Create S3 buckets . Configure access policies to S3 buckets . Enable encryption on S3 buckets . Configure data lifecycle policies (expiration, move to Glacier, change Storage Tier, etc.) . Enable access logging
Service Limitation	

Table 5 Amazon S3

Amazon Glacier	
Overview	Amazon Glacier is a file storage service that provides storage for data archiving and long-term backup.
Setup Activities	. Create Vaults . Setup data retrieval policies
Service Request	. Create Vaults . Start an archive retrieval job
Service Limitation	

Table 6 Amazon Glacier

Amazon Route 53	
Overview	Amazon Route 53 is a scalable domain name system
Setup Activities	. Setup of hosted zones . Setup of dns records in managed hosted zones . Setup health check monitors for specific dns records . Setup private VPC name resolution
Service Request	. Setup and modification of hosted zones . Setup and modification of dns records . Setup and modification of health check monitors for dns records
Service Limitation	. Design of platform name resolution architecture

Table 7 Amazon Route 53

AWS VPN Gateway	
Overview	IPSEC VPN connections from VPCs (or Transit Gateway) to on-premises network
Setup Activities	. Create Client gateway . Create target gateway . Configure VPC route tables
Service Request	. Reset tunnels . Changes to VPN gateway already created . Change VPC route tables
Service Limitation	. On-premises device configuration for unmanaged devices . Design of WAN architecture . Client-to-Site VPNs

Table 8 VPN Gateway

AWS Identity and Access Management (IAM)	
Overview	AWS IAM allows secure access management to services and resources
Setup Activities	. Creation of Groups . Creation of Roles . Creation of Users . Creation of Policies . Creation of Password policies
Service Request	. Create, change or delete Groups . Create, change or delete Roles . Create, change or delete Users . Create, change or delete Policies . Create, change or delete Password policies
Service Limitation	. User lifecycle for Client access must be agreed and done via an external authentication provider

Table 9 AWS IAM

AWS Key Management Service (KMS)	
Overview	AWS Key Management Service (KMS) is an encryption and key management service scaled for the cloud. KMS keys and functionality are used by other AWS services, and the Client can use them to protect data in its own applications that use AWS.
Setup Activities	. Create ClientMaster Keys (CMK) . Setup access control to CMK
Service Request	. Create CMK . Manage access control to CMK . Enable/disable CMK

AWS Key Management Service (KMS)	
	. Rotate CMK . Delete CMK
Service Limitation	. AWS Managed keys are included in Region pricing. This item is required when additional CMK are to be managed.

Table 10 AWS KMS

AWS Certificate Manager (ACM)	
Overview	AWS Certificate Manager (ACM) makes it easy to provision, manage, and deploy SSL/TLS certificates on AWS managed resources.
Setup Activities	. Request new public certificate . Validate domain ownership (via DNS validation on managed domains) . Delete certificates . Import self-signed or public CA signed certificates
Service Request	. Request new public certificate . Validate domain ownership (via DNS validation on managed domains) . Delete certificates . Import self-signed or public CA signed certificates
Service Limitation	. AWS ACM Private CA service is not included as part of this service and are out of scope . All certificates created will be automatically renewed

Table 11 AWS ACM

AWS Secrets Manager	
Overview	AWS Secrets Manager helps to securely encrypt, store, and retrieve credentials for databases and other services.
Setup Activities	. Create, delete, restore secrets . Setup VPC Secrets Endpoint
Service Request	. Create, delete, restore secrets . Secret rotation . Setup VPC Secrets Endpoint
Service Limitation	. Secrets Manager is used as an integral part of the managed service to store passwords. . Secret rotation only available on secrets used by services covered in this service description. 3rd party or application related secret rotation is out of scope.

Table 12 AWS Secrets Manager

AWS License Manager	
Overview	AWS License Manager streamlines the process of bringing software vendor licenses to the AWS Cloud
Setup Activities	. Add license configuration . Configure license rules . License association/disassociation . Create a report generator
Service Request	. Add license configuration . Configure license rules . License association/disassociation . Create a report generator
Service Limitation	. Client must provide detailed license configuration parameters . Client must provide detailed license rule configuration . Client is responsible of correct license usage . Client is responsible of License Manager report checking. Reports are not part of SDM role. . Only servers on AWS are supported. No on-promises inventory support is included.

Table 13 AWS License Manager

AWS CloudWatch	
Overview	Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications run on AWS.
Setup Activities	. Creation of log groups . Creation of alerts to complement NTT monitoring tool . Setup of event driven actions not part of a full serverless or event-driven architecture
Service Request	. Creation and management of log groups . Creation and management of alerts to complement NTT monitoring tool . Setup and management of event driven actions not part of a full serverless or event-driven architecture
Service Limitation	. Creation of additional custom alarms is out of scope and will require additional Professional Services scoped to cover it. Alerts generated by custom alarms will be sent to Client's recipients . Creation of dashboards is out of scope for this managed service. Custom dashboard creation will require Professional Services to be quoted. . Container Insights and Lambda Insights monitoring is out of scope of this service . Cloudwatch RUM is out of scope of this service . APM using CloudWatch is out of scope of this service

Table 14 AWS CloudWatch

AWS CloudHSM	
Overview	AWS CloudHSM offers secure cryptographic key storage for Clients by providing managed hardware security modules in the AWS Cloud.
Setup Activities	. Setup clusters . Setup backups . Creation of HSM users
Service Request	. Add or remove additional HSM in a cluster . Restore a cluster from backup . Delete a cluster . Manage HSM Users . Manage HSM Keys
Service Limitation	.

Table 15 AWS CloudHSM

1.6 Managed Infrastructure Services (Networking)

(a) PaaS and SaaS Networking

(i) Overview

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

(ii) Supported Technologies

- Amazon CloudFront
- Elastic Load Balancing
- AWS Transit Gateway

Amazon CloudFront	
Overview	Global content delivery network service
Setup Activities	. Create distributions . Configure Client provided cache policies . Configure managed cache policies

Amazon CloudFront	
Service Request	. Change Client provided cache policies . Change managed cache policies . Invalidation requests
Service Limitation	. Creation of CloudFront policies is limited as it's highly dependent on underlying application

Table 16 Amazon CloudFront

Elastic Load Balancing	
Overview	Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones.
Setup Activities	. Create target groups . Create listeners . Create Load Balancers (Application, Network or Classic supported) . Create routing rules (as per Client Application requirements)
Service Request	. Create, change or delete Target Groups . Create, change or delete Listeners . Create, change or delete routing rules
Service Limitation	. Limited support to Gateway Load Balancers

Table 17 Elastic Load Balancing

AWS Transit Gateway	
Overview	AWS Transit Gateway connects VPCs and on-premises networks through a central hub.
Setup Activities	. Create VPC attachments . Create VPN attachments . Create Direct Connect attachments . Create peering connection to other Transit Gateway . Create route tables
Service Request	. Create, change or delete route tables . Create, change or delete VPC attachments . Create, change or delete VPN attachments . Create, change or delete peering connection
Service Limitation	. On-premises device configuration for unmanaged devices . Design of WAN architecture

Table 18 AWS Transit Gateway

(b) PaaS and SaaS Security

(i) Overview

This element of the service covers the configuration, monitoring and management of 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

- AWS WAF

AWS WAF	
Overview	AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions or an Application Load Balancer. Client can also use AWS WAF to block or allow requests based on conditions that it specifies, such as the IP addresses that requests originate from or values in the requests.
Setup Activities	. Apply defined web access control lists (web acl) . Apply defined rules and rule groups

AWS WAF	
	. Apply AWS Managed Rules . Apply customized web requests and responses
Service Request	. Apply, change or delete defined web access control lists (web acl) . Apply, change or delete defined rules and rule groups . Apply, change or delete AWS Managed Rules . Apply, change or delete customized web requests and responses
Service Limitation	. Rule definition is not included. Client or 3rd party can provide rules, or additional Professional Services can be requested to help the Client with rule creation.

Table 19 AWS WAF

Amazon Inspector	
Overview	Amazon Inspector is a security vulnerability assessment service that helps improve the security and compliance of your AWS resources.
Setup Activities	. Installation of Amazon Inspector agent (only on managed OS) . Create assessment target . Create assessment templates . Schedule assessment runs (via Lambda) . Integration with SecurityHub
Service Request	. Installation of Amazon Inspector agent (only on managed OS) . Create, delete assessment target . Create, delete assessment templates . Schedule assessment runs (via Lambda) . Monthly assessment reports (only when Compliance Manager service is contracted)
Service Limitation	. Installation of Amazon Inspector agent is only performed on managed instances OS or ASG AMIs . Assessment templates should be defined by the Client or SOC . All assessment runs notification require a SOC recipient to review, process and ask for specific remediations. Alert review is out of scope. . Monthly assessment report review is included when Compliance Manager service is contracted

Table 20 Amazon Inspector

Amazon GuardDuty	
Overview	Amazon GuardDuty is a continuous security monitoring service. Amazon GuardDuty can help to identify some unexpected and potentially unauthorized or malicious activity in Clients AWS environment.
Setup Activities	. Enable GuardDuty . Add suppression rules (Client must provide the required suppresion rules)
Service Request	. Update trusted IP and threat lists (when provided manually by the Client) . Add suppression rules (Client must provide the required suppresion rules) . Suspend or disable GuardDuty . Monthly findings review (only when Compliance Manager is contracted)
Service Limitation	. All findings should be sent to a SOC for review and action. SOC capabilities is out of scope of this service. . Remediations are only applicable to those services under management . The service will be enabled at AWS Organizations level . It is recommended to integrate the service with AWS Security Hub.

Table 21 Amazon GuardDuty

AWS Security Hub	
Overview	AWS Security Hub provides you with a comprehensive view of the security state of Client AWS resources. Security Hub collects security data from across AWS accounts and services, and helps the Client analyze your security trends to identify and prioritize the security issues across your AWS environment.

AWS Security Hub	
Setup Activities	. Security Hub activation in AWS Organization . Enabling of managed security standards . Create custom insights
Service Request	. Enabling of managed security standards . Create custom insights
Service Limitation	. The service can only be managed when the Client landing zone is managed via AWS Organizations. . Additional SOC service is required to retrieve and analyze any finding and report any required remediation on the affected service. . Definition of custom insights is out of scope of the service. . Reporting on findings is out of scope of the service. A SOC service is required if findings have to be treated and actioned upon. . Remediations on findings have to be requested for the affected service when that service is included as part of the NTT scope of management. No remediation can be applied on services not managed by NTT.

Table 22 AWS Security Hub

(c) Cloud Direct Connectivity

(i) Overview

This element of the service covers the configuration, monitoring and management of AWS Direct Connect. Charges are based on the number of Direct Connect connections as specified in the SOW.

(ii) Supported Technologies

- AWS Direct Connect

AWS Direct Connect	
Overview	AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable.
Setup Activities	. Create a new connection . Create required virtual interfaces . Configure routing . Create LAGs (Link Aggregation Group)
Service Request	. Change or delete virtual interfaces
Service Limitation	. On premises endpoint setup and management not included

Table 23 AWS Direct Connect

1.7 Managed Infrastructure Services (Compute)

(a) IaaS Scaling Group (Elastic)

(i) Overview

This element of the service covers the configuration, monitoring and management of elastic scaling groups. Charges are based on the number of scaling groups as specified in the SOW, regardless of the number of VMs that may be running during a certain period of time all VM's must be included in charges.

(ii) Supported Technologies

- Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling	
Overview	Scale compute capacity to meet demand
Setup Activities	. Create launch template . Create auto scaling group . Setup scaling plan . Setup scaling policies . Create elastic load balancer . Creation of security group

Amazon EC2 Auto Scaling	
Service Request	. Manual trigger of instance refresh . Manual trigger of up or down scale actions . Modify launch template . Modify auto scaling group . Modify auto scaling policies . Modify security group rules
Service Limitation	. Does not include the management of the OS or services in the auto scaling group which must be added to the SOW specifically as In Scope otherwise it is out of scope.

Table 24 Amazon EC2 Auto Scaling

(b) IaaS- VM (Static)

(i) Overview

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

(ii) Supported Technologies

- Amazon EC2

Amazon Elastic Compute Cloud (EC2)	
Overview	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity to build and host software systems.
Setup Activities	. Deploy EC2 instance . Create security groups . Create AMI (when OS and above layers are managed) . Resource tagging . Create instance profile and role
Service Request	. Change instance type . Change volume sizes . Add additional volumes . Update AMI (when OS and above layers are managed) . Manage tags . Deployment of additional non-managed instances . Manage associated IAM roles and instance profile
Service Limitation	. Does not include management of OS and any additional services running in the instance which must be added to the SOW specifically as In Scope otherwise it is out of scope

Table 25 Amazon EC2

1.8 Managed Infrastructure Services (Storage)

(a) Cloud PaaS File Storage

(i) Overview

This element of the service covers the configuration, monitoring and management of Amazon EFS and Amazon FSx. Charges are based on the number of instances present in the environment.

(ii) Supported Technologies

- Amazon EFS
- Amazon FSx for Windows File Server

Amazon Elastic File System (Amazon EFS)	
Overview	Fully managed file system for EC2 on NFS protocol
Setup Activities	. Create a file system . Create mount targets . Create security groups . Create file system policy . Create access points . Create backup job

Amazon Elastic File System (Amazon EFS)	
Service Request	. Modify file system's settings . Modify storage class . Modify security groups . Modify file system policy . Modify access points . Modify backup schedule . Backup restoration
Service Limitation	. Client configuration is not included in the service and is out of scope. Additional relevant managed services should be quoted.

Table 26 Amazon EFS

Amazon FSx for Windows File Server	
Overview	Fully managed Windows native file system using SMB protocol
Setup Activities	. Create a file share . Setup file share backup . File share mapping (only on managed OS) . Setup authentication via managed Active Directory . Setup file share backups
Service Request	. Modify a file share . Restore file system from backup . Configure DNS aliases . Manage user sessions . Manage data deduplication . Manage storage quotas . Manage shadow copies
Service Limitation	. File share mapping is only included when the target OS is also managed which must be added to the SOW specifically as In Scope otherwise it is out of scope.

Table 27 Amazon FSx for Windows File Server

(b) Cloud Identity & Domain

(i) Overview

This element of the service covers the configuration, monitoring and management of Cloud Identity services. Charges are based on the number of instances present in the environment as specified in the SOW.

(ii) Supported Technologies

- AWS Directory Services
- AWS Single Sign-On

AWS Directory Service	
Overview	AWS Directory Service provides multiple ways to set up and run Microsoft Active Directory with other AWS services such as Amazon EC2, Amazon RDS for SQL Server, Amazon FSx for Windows File Server, and AWS Single-Sign On. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use a managed Active Directory in the AWS Cloud.
Setup Activities	. Create AD Connector . Create Simple AD . Create groups, users and policies . Join EC2 instances
Service Request	. Change or delete an AD Connector . Change or delete a Simple AD . Manage groups, users and policies . Manage joined EC2 instances
Service Limitation	. AWS Managed Microsoft AD is limited to on-cloud only AD solutions. In case of additional domains to be joined in a forest or to establish trust relationships an AD on-IaaS deployment is mandatory.

Table 28 AWS Directory Service

AWS Single Sign-On	
Overview	AWS Single Sign-On (AWS SSO) is a cloud-based service that simplifies managing SSO access to AWS accounts and business applications.
Setup Activities	. Manage users and groups . Connect Microsoft AD or other supported external identity provider . Setup permission sets . Enable MFA
Service Request	. Manage users and groups . Assign User access and permission sets . Setup and update permission sets . User MFA setup (MFA serial code will be provided to users)
Service Limitation	. Configuration of the 3rd party cloud apps using AWS SSO is out of scope. NTT will still be in charge of providing configuration details and configure the AWS side of the configuration . AWS SSO MFA is only supported when using SSO identity store, Microsoft AD or AD connector.

Table 29 AWS Single Sign-On

(c) Cloud Hybrid Identity

(i) Overview

This element of the service covers the configuration, monitoring and management of Cloud Identity services. Charges are based on the number of instances present in the environment as specified in the SOW.

(ii) Supported Technologies

- AWS Cognito

Amazon Cognito	
Overview	Amazon Cognito handles user authentication and authorization for your web and mobile apps.
Setup Activities	. Setup access to manage user pools and identity pools . Create user pool . Add App Client to user pool (as per Client requirements) . Setup custom domain for App Client . Setup 3rd party identity providers in user pool . User management . Setup Identity Pools
Service Request	. Manage user and identity pools . Add, modify, delete App Client configuration . Add, modify, delete 3rd party identity providers
Service Limitation	. Built-in webpage customization must be provided by the Client . 3rd party identity provider configuration is out of scope . Lambda trigger code development is out of scope of the service . Client can be given access to manage user and identity pools if they require so . Client application codebase development is out of scope

Table 30 Amazon Cognito

1.9 Managed Data Protection

(a) AWS Backup

(i) Overview

This element of the service covers the configuration, monitoring, and management of AWS Backup. Charges are based on the number of regions where managed resources are protected, regardless of the number of VMs protected as specified in the SOW.

(ii) Supported Technologies

- AWS Backup

AWS Backup	
Overview	AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises.
Setup Activities	. Creation of backup vaults . Creation of backup plans
Service Request	. Creation and management of backup vaults . Create a backup plan . Update a backup plan . Initiate on-demand backup . Restore a backup . Creation of cross-region copies . Creation of cross-account copies
Available Monitors	. Backup job status
Service Limitation	. On tag based plans, resource tagging is only included when those resources are under management. . Centralised backup management is only available to the AWS services that AWS Backup supports.

Table 31 AWS Backup

1.10 Disclaimer

Please note that Service Requests and monitors described in this service description represent only a sample and are subject to change due the rapidly evolving offering from Amazon Web Services.

Monitors are subject to change as per the Service Improvement Process.

All activities are subject to the AWS online terms, the Agreement, and limitations provided by the agreement Client is using to procure the AWS environment.