For: GATI . Acct#: 5892858
Opportunity #: 4516996
Rackspace Sales Rep./Account Manager: Bhuvnesh Soni
Pricing and Terms Valid to: 29/09/2023

STATEMENT OF WORK FOR PROFESSIONAL & CONSULTING SERVICES

Project title: GEMS: AWS Design and Implementation Services.

Prepared for: GATI EXPRESS & SUPPLY CHAIN PRIVATE LIMITED

This Statement of Work for Professional and Consulting Services ("**SOW**") is between the Rackspace entity and the customer signing below ("**Rackspace**" and "**Customer**" respectively). This SOW is subject to and governed by the Master Services Agreement located at https://www.rackspace.com/information/legal/MSA and the Professional & Consulting Services Terms at https://www.rackspace.com/information/legal/PSTerms. The Professional & Consulting Services Scoping Document at Schedule 1 is incorporated in this SOW.

The Agreement constitutes the complete and exclusive agreement between the parties regarding the subject matter and supersedes and replaces any prior understanding or communication, written or oral. The individual signing represents to Rackspace that they are authorized to sign on behalf of Customer. Customer accepts the terms of the Agreement, including any document or terms referenced above.

Accepted by Customer (All Fields Required)		**Accepted by Rackspace International GmbH**	
Signature:	Kapil Mahajan	Signature:	
Date:	29 September 2023	Date:	
Name:	Kapil	Name:	
Title:	GCITO	Title:	
Company:	Gati & Allcargo supply Chain pvt ltd	Company:	**Rackspace International GmbH**

SCHEDULE 1
PROFESSIONAL & CONSULTING SERVICES

1. EXECUTIVE SUMMARY. Gati Limited is an Indian logistics company, headquartered in Hyderabad, Telangana. It offers surface and air express logistics, warehousing and supply chain, air freight and e-commerce services. Gati has offices in all major states of India. Gati was founded in 1989 and first started operations between Madras (now Chennai) and Madurai. In 2020, it was acquired by Allcargo Logistics. Gati is listed on the National Stock Exchange and Bombay Stock Exchange.

GATI seeks the commercial responses from Rackspace for setup and maintenance of AWS Infrastructure services for Digital transformation initiatives that we are embarking across AllCargo Group entities, also Allcargo wants to develop a scalable Data Lake platform for their GATI and ACL data centres for all their analytical applications.

Current scope is limited to GEMS2.0 Platform for GATI Limited

Rackspace follows AWS best practice guidance for cloud and will work alongside Customer teams to execute discovery and design an AWS strategy that adheres to internal and external security, governance and compliance requirements and establish an approach for continuous compliance that ensures all AWS environments are monitored and workloads are running as designed. The Rackspace professional services team shall assist Customer within the scope of services defined in this SOW.

2. BUSINESS HOURS. Business hours for performance of this SOW are Monday through Friday 9 am to 6 PM IST (excluding public holidays).

3. SOW TERM. The services under this SOW are for a fixed term as set out below.

4. RACKSPACE RESPONSIBILITIES.

4.1. Scope of Services. Rackspace shall provide the Services as set out in this SOW under a project having the following phases:

(A) Phase 0: Resource Mobilization

(i) Total Estimated duration. Within ten Business Days of SOW execution, if not sooner.

(ii) Activities Description. Mobilization of Rackspace Resources.

(B) Phase 1 – Discovery, Establishment & Governance

(i) Activities Description.

(a) Project Initiation

- The Project Manager will engage with the Customer to confirm scope and begin scheduling of subsequent activities. Activities as part of Project Initiation include:
- Welcome email.
- Confirmation of project scope
- Confirmation of customer stakeholders
- Scheduling of activities
- Cloud account preparation and details
- Project outline / reports schedule and timelines

(b) Establish governance framework.

- Define frequency of regular governance meetings and attendees.
- Define decision making process and stakeholders.
- Identify internal and external dependencies.
- Identify critical path and milestones.
- Risk analysis and impact assessment
- Define comms plan & business stakeholder critical check points.
- Review environments as-is, identify future deployment process and operating model, provide gap analysis.

(c) Discovery and planning.

- Remote discovery workshop sessions will be scheduled between the Rackspace Architect and Customer. The Customer's technical teams (architecture, data, and security) will be required to attend the workshop to ensure representation of the relevant parties.
- Conduct discovery on requirements for security and compliance.
    - Organization Design, Service Control Policies and Config.
    - Identify workload isolation needs for business unit and/or regulatory requirements.
    - Establish target security baselines for AWS accounts.
    - Identify ALLCARGO Security Standards/Requirements
        - Encryption
        - SCPs
        - Firewalls
        - Authentication, Authorization, Access
        - Auditability
    - Conduct discovery on compliance requirements.
    - Understand documentation requirements.
    - Understand requirements for proving compliance have been met.
- Conduct discovery on requirements for logging, monitoring, and tagging.
    - Identify requirements for post-implementation logging using AWS cloud-native services.
    - Identify requirements for post-implementation monitoring using AWS cloud-native services.
    - Identify requirements for post-implementation logging using AWS cloud-native services.
    - Log retention requirements
    -

(C) Phase 2 -Design & Planning

(i) Activities Description.

A. Infrastructure Design

(a) The Rackspace Solution Architect will conduct solution workshops and prepare the Detailed Design for implementation.

- Review the customers' existing architecture and propose future state architecture in compliance with AWS Best practices on Security, reliability, Performance, Operations and Cost Optimization.
- Advise customer with the high-level future state architecture on AWS with networks, compute, database, storage, and security.
- Create an entity-wise Organization set-up.

- Build production environment(s) with multi availability zones and DR site using Terraform/CloudFormation scripts for HA and resilience.
- Compliance to our standards and guidelines w.r.t Technology, Infrastructure, Network Topology and Security
- Conduct discovery and advise on requirements for AWS Control Tower Blueprint or for bespoke foundational infrastructure, landing zone, or equivalent “cloud ready environment!
- Rackspace will take information gathered from the workshop session and revalidate the High-Level Design (HLD) diagram previously prepared. The HLD defines a recommended network (if applicable) and account/OU structure (if applicable) aligned to well-architected best practices.
- Develop architecture and implementation plan for AWS Foundation
- Develop backup plan(s) and associated automation needs.
- This LLD will be provided to the Customer for review (up to two (2) review update cycles) and approval before implementation can begin.

(b) The Solution Architect will prepare a Detailed Design (DD), that will contain the necessary information to build the AWS environment, including:

(c) Establish target technical standards for AWS accounts.

- Frameworks & standards
- AWS Well-Architected recommendations
- CIS Controls

(d) Incorporate Customer security standards.

- Establish encryption at rest and in transit requirements.
- Draft operational roles and permissions
- Identify operational role expectations, such as not logging into servers to make manual config changes.
- Setup and configure AWS guardrails (SCP and Configs) on the respective OUs for security baseline and governance.

(e) Review AWS foundation requirements

- Account strategy - Core Organizational Unit: Master Account, Security and Log Archive Accounts
- Networking/VPC requirements and VPC structures within AWS accounts
- DNS
- Interconnectivity (VPN / Direct Connect / RackConnect, Transit Gateway/NAT)

(f) Security and compliance requirements

- AWS Config CIS Benchmark
- Map security tool requirements to AWS native solutions
- Identify continuous compliance requirements using AWS Config.
- Document security standards

(g) Identity & access (IAM) integration

(h) LDAP/Active Directory

(i) Advice GATI on Identity and Access Management (IAM) best practices

- Policies to limit AWS deployments based on services.
- Policies to limit users based on roles/group policies.
- Review 2FA requirements for IAM users and infrastructure access

(j) Network Account & VPC

- AWS transit gateway attachment and config.
- Increase traffic inspection through AWS Network firewall.
- North-south networking (Internet Ingress & Egress)
- Internet Ingress VPC in Network Account

- AWS Network Firewall Design, Implementation, Integration
- Local and Global Load Balancer- (AWS Native options available)
- Cloud front.

- Internet Egress VPC in Network Account
  - AWS Network Firewall Design, Implementation, Integration
- North-south networking between on-premises and AWS
  - Review & Design key components: ALB, WAF, CloudFront, GuardDuty, Config, CloudWatch, CloudTrail, route53, VPC, TGW.

(k) Shared services Account

- Active Directory
  - Rackspace will provision the EC2 instances for the Active directory on-premises integration.
  - Setup and configure Shared Services account and VPC to deploy common services such as Active Directory Domain Controller instances.
  - Setup and configure Route53 for public and private hosted zones.
- Backup & Restore
  - Design of AWS Native backup solution
  - Native AWS backup on infra level.
  - Backup to performed on for Kubernetes clusters and all services we are provisioning like codecommit, API gateway, S3, DBs, EC2s, RDS as applicable etc.
  - Native AWS restore on AWB backup runbook.
- Logging and monitoring
  - Review data sources
  - Review existing tools/methodologies and use cases.
  - Establish & document strategic direction.
  - Cross region replication options wherever applicable.
- Tagging strategy
  - Customer tagging requirements
  - MAP tagging requirements.

(l) Workload Account - Application

- Non-Prod and Prod workload account
- Terraform implementation of underlying AWS Infrastructure
- EC2//RDS/S3/ELB
- VPC & ALB Implementation to support Application Workloads

(m) Disaster Recovery (DR) Strategy

- Overall DR strategy/requirements at an infrastructure level.
- Design and document requirements for multi-AZ / Multi region DR plan.
- Pilot light strategy for DR in another region (Customer will confirm the region)
- Document of RTO/RPO

(n) Other AWS services

- WAF deployments
- Security groups
- ACLS
- Auditability
- Automation requirements
- Infrastructure deployments
- Application deployments
- Logging/Monitoring requirements
- Associated AWS services

- AWS SSO
- AWS Config
- AWS Service Catalog
- AWS CloudWatch
- AWS CloudTrail
- AWS S3 for Log aggregation
- Route53
- Global accelerator
- Load Balancers'
- EKS, with metrics server, HPA, RBAC
- EKS Kube2IAM for accessing other AWS services from EKS.
- Install Istio on Kubernetes, with Grafana Prometheus, Kiali, Jaeger
- Aurora PostgreSQL DBs
- AWS ElastiCache Redis
- AWS MSK
- CloudWatch setup
- API gateway
- Cognito
- S3
- Cloud trail
- Setting up private connectivity with on-prem DC.

(o) LZ Well Architected report

B. Devsecops Design.

(a) Deliver 1-day Devops, automation, CI/CD workshop. for Infrastructure automation, environment operation.

(b) Design the Intelligent Devsecops platform using chain-off tools (open source) with an ability to handle the developer's workloads for CI/CD build, and automatic quality checks, notifications/alerts, Quality Dashboards & etc.

(c) Requirements for deploying Infrastructure as Code (IaC)

(d) Current and desired state of tools for application deployment

(e) CI/CD Pipelines

(f) Target pipeline and orchestrator platforms

(g) Infrastructure as code executor leveraged by pipelines:

- Terraform / CDK
- DevOps tools are Jenkins, SonarQube, Clair, selenium, JMeter, Nexus, Device Farm GIT, Container registry and AWS code commit for code commit.
- Identify requirements for additional AWS services to implemented.

(D) Phase 3: Implementation and testing.

(i) Activities Description.

A. Infrastructure Build

(a) Build and deploy AWS Foundation via automated pipeline to production and non-production environments.

(b) Deploy landing zone as defined in the Detailed Design.

(c) Build and deploy resource components and logical grouping as defined in the Detailed Design.

- Deploy network connectivity and security configuration.
- Setting up OUs as per defined and approved categorization for instance by environment or department
- Setup and configure hub and spoke network topology using Transit Gateway for VPC attachments.
- Build and deploy AWS Foundation via terraform IaC to non-production environments.
- Configure and deploy backup automation in non-production and production accounts.

(d) DEV Environment provisioning by Terraform.

- Setup up and configure the following resources for the Dev environment for gems>
- Setup and configure 1 EKS cluster with Autoscaling and spot instances (Ex.m5. xlarge)
- Setup and configure 1 RDS instance (ex: r5. large)
- Setup and configure AWS Managed Streaming Kafka (MSK)cluster.
- Setup and configure AWS Managed ElastiCache for Redis cluster.
- Test the functionality and handover the infra to the vendor team to install and test the application.

(e) SIT Environment provisioning by Terraform.

- Setup and configure the following resources for the Dev environment for GEMS.
- Setup and configure 1 EKS cluster with Autoscaling and spot instances (Ex.m5. xlarge)
- Setup and configure 1 RDS instance (ex: r5. large)
- Setup and configure AWS Managed Streaming Kafka (MSK)cluster.
- Setup and configure AWS Managed ElastiCache for Redis cluster.
- Test the functionality and handover the infra to the vendor team to install and test the application.

(f) UAT Environment provisioning by Terraform.

- Setup up and configure the following resources for the GEMS UAT
- Setup and configure 1 EKS cluster with Autoscaling and spot instances (Ex.m5. xlarge)
- Setup and configure 4 RDS instance (ex: r5. large)
- Setup and configure AWS Managed Streaming Kafka (MSK)cluster.
- Setup and configure AWS Managed ElastiCache for Redis cluster.
- Test the functionality and handover the infra to the vendor team to install and test the application.

(g) PROD Environment provisioning by Terraform.

- Setup up and configure the following resources for the GEMS Prod
- Setup and configure 1 EKS cluster with Autoscaling and spot instances (Ex.m5. xlarge)
- Setup and configure 4 RDS instance (ex: r5. large)
- Setup and configure AWS Managed Streaming Kafka (MSK)cluster.
- Setup and configure AWS Managed ElastiCache for Redis cluster.
- Test the functionality and handover the infra to the vendor team to install and test the application.

(h) MDM and Spotfire Test Environment provisioning by Terraform.

- Setup New VPC for MDM and Spotfire test environment
- Setup up and configure the following resources for the MDM and Spotfire for GEMS.
- Setup and configure 5 EC2 instance for Test Environment.
- Setup and configure 1 RDS instance for PostgreSQL (ex: r5.2xlarge)
- Test the functionality and handover the infra to the vendor team to install and test the application.

(i) MDM and Spotfire Production Environment provisioning by Terraform.

- Setup New VPC for MDM and Spotfire environment
- Setup up and configure the following resources for the MDM and Spotfire for GEMS.
- Setup and configure 1 EC2 instance for Spotfire Server and Spotfire Node Manager
- Setup and configure 2 EC2 instances for Business Works and MDM.
- Setup and configure 1 EC2 instance for EMS and TEA.
- Setup and configure 1 RDS instance for PostgreSQL (ex: r5.2xlarge)
- Test the functionality and handover the infra to the vendor team to install and test the application.

(j) Disaster Recovery (DR)

- Setup DR VPC in another region
- Setup RDS replica in DR region
- Setup the DR subnet and provision the DR application resources running on EKS, ALB, Route 53, KMS using Terraform scripts for deployment.
- Perform failover test to the DR region and document the RTO/RPO.

(k) Security Control Implementation

- AWS Organization Design & Policies
- High Level Security and Compliance design according to customer standards.
- IAM Policies & Access Levels
- Key Policies
- AWS security implementation is based on AWS security design guidelines and customer existing compliance standards.
- Setup and configure AWS CloudTrail's, CloudWatch, VPC Flow logs and DNS logs to the centralized Log Archive accounts for consolidation.
- Enable applicable conformance packs in AWS Config for ongoing security best practice review.
- Set up and configure AWS GuardDuty for threat detection on all applicable AWS OU accounts.
- Setup and configure the following AWS security services.
- WAF rules setup and CloudFront
- Security Hub
- IAM roles and policies
- KMS
- Secret Manager
- Certificate Manager
- CloudWatch
- CloudTrail
- S3 logging/Archiving

(l) Perform Well architected review (WAR) for the Landing Zone environment.

B. Devsecops Implementation.

(a) Setup and run the Intelligent Devsecops platform using chain-off tools (open source) with an ability to handle the developer's workloads for CI/CD build, and automatic quality checks, notifications/alerts, Quality Dashboards & etc.

(b) DevOps tools are Jenkins, SonarQube, Clair, selenium, JMeter, Nexus, Device Farm GIT, Container registry and AWS code commit for code commit.

- Install and Configure Jenkins: with Master and configure Auto scaling for Slave, which will add the server automatically based on metrics/threshold defined.
- Set up initial configuration, including security settings, plugins, and system configurations.
- Install Required Plugins:
- Configure Global Tools: tools like Git, JMeter, and Selenium, configure them as Global Tools in Jenkins to make them available across all projects.
- Create a new Jenkins pipeline for different AWS environments (Dev, SIT, UAT and Prod) for Gems Application.
- Define pipeline stages.
- Integrate with sonar cube, Clair, Selenium, JMeter, Nexus and container registry.
- Provision and Integrate with Document Management software (DMS) toolset (If required).
- Provision and Integrate with Camunda for business process automation toolset (If required).
- Integrate with Git/AWS code commit for version control.
- Integrate with device farm for mobile testing.
- Configure notifications and reporting.
- Setup OpenVPN to secure private access to Dev team during development.
- Test and iterate: Test your pipeline thoroughly for one (1) environment (Ex: Dev) with sample projects and iterate as needed to fix any issues and handover the details to All cargo developers' team for further enhancement.

(E) Phase 4 – Enterprise Datalake services

Rackspace will provide the following Datalake scope of services via Rackspace 3rd party vendor.

(i) Activities Description.

A. Requirement gathering and Infrastructure setup.

(a) Requirement gathering
- AWS account access management & user creation
- Table structure understanding and Transformation logic documentation.

(b) BRD and FRD Documents.
- Create design, BRD, FRD documents.
- Business signs off

(c) Infrastructure Setup
- Setup AWS infrastructure
- Establishing data source & network connections with data centres.

B. Datalake

(a) Development
- Setup DMS continuous replication jobs to migrate tables to raw layer.
- Create glue crawlers & data catalogs.
- Implement CDC logic to monitor and implement changes to curated layer.
- Setup Governance & failure alerts

(b) Validation & Testing
- Testing & Jobs Monitoring
- Validation & UAT of the data migrated.

(c) Governance Setup and Data Archival.
- Reviewing audit & logging policies

C. Go-Live and Documentation

(a) Automation and go live.
- Automation & scheduling
- Production release

(b) Documentation of Architecture
- Documentation (Data Dictionary, User guide & FAQs)

D. Scope of services.

(a) Movement of 1973 tables from GATI & ACL data centres to AWS S3 using AWS DMS

(b) CDC implementation for capturing changes from respective source data centre and replicating the same in the Data Lake

(c) CDC implementation for capturing changes from the S3 and replicating the same in staging layer of the source data centres

(d) Manage Data Catalog using AWS Glue Data Catalog & Crawlers.

E. Key Project Deliverables

(a) Data Lake on AWS S3

(b) Requirement gathering and design document for plan of action

(c) Data validation documentation & Daily migration reports

(d) Designing future state architecture and consultation on technology stack, data governance & security

(e) User guide and documentation of the production system design and configuration

F. Project Plan and RACI Matrix.

(a) 2 Data centres (GATI + ACL) will be migrated to data lake on S3 in 4 weeks

(b) AWS DMS will be used to connect to the data centres and migrate data from source data centres to target raw S3 layer.

- Larger DMS instances to be used during full load migration.

- Smaller DMS instances to be used for on-going replication.

(c) AWS DMS will be used to capture the transaction logs (CDC)

(d) Amazon EMR will be used to capture the CDC logs and replicate the changes in the curated S3 layer.

(e) Glue crawler and catalog will be used to crawl data and maintain meta data of both raw and curated layer.

(f) Summary of Milestones & Deliverables

Milestone	Tasks	Sub Tasks	W1	W2	W3	W4
Requirement gathering and Infrastructure setup	Requirement gathering	AWS account access management & user creation				
		Table structure understanding and Transformation logic documentation				
	BRD & FRD documents	Create design, BRD, FRD documents				
		Business signs off				
	Infrastructure setup	Setup AWS infrastructure				
		Establishing data source & network connections with data centres				
Data Lake	Development	Setup DMS continuous replication jobs to migrate tables to raw layer				
		Create glue crawlers & data catalogs				
		Implement CDC logic to monitor and implement changes to curated layer				
		Setup Governance & failure alerts				
	Validation & Testing	Testing & Jobs Monitoring				
		Validation & UAT of the data migrated				
	Governance setup & data archival	Reviewing audit & logging policies				
Go-Live	Automation and go live	Automation & scheduling				
		Production release				
Documentation	Documentation of architecture	Documentation (Data Dictionary, User guide & FAQs)				

(g) RACI Matrix:

	Business	IT Team	Project Manager	Solution Architect	Data Engineer
Tasks	**Customer team**		**Rackspace 3rd Party Vendor**		
Requirement gathering	R	C	A		R
Establishing private network with data sources		R	A	R	
Infrastructure setup	I	R/C		R/A	
Data Lake Development			I	A	R
Validation & Testing	C		A		R
Deployment automation				C	A
Governance setup and data archival				C	A
Production release			A		R
Documentation of requirement understanding, transformation logics and data dictionary			A		R

(F) Phase 5 – Knowledge transfer and Project Closure

(i) Activities Description.

(a) A final workshop will be held with the customer to handover the environment post-implementation, to confirm that any outstanding issues have been resolved and to provide relevant knowledge transfer to the customer.

(b) Handover, Knowledge Transfer and Project Closure

• Rackspace Architect will work through the handover activities required for Customer or Managed services partner to assume control of the new environment.

(c) Documentation updates / finalization.

(d) At the conclusion of this workshop, the project manager will close the project, and provide the Project Closure Report.

(e) The Customer will be required to provide formal project sign-off within five (5) calendar days from formal notification. If no formal feedback is provided by the Customer within this period, the project will be deemed closed.

4.2. Deliverables. In connection with the Services, Rackspace shall work to achieve or provide the following Deliverables:

(A) Detailed Design - A Rackspace document that contains the necessary information to build the Customer Target Environment.

(B) DR Runbook– A Rackspace document that contains Disaster recovery orchestration steps and sequence of events.

(C) All diagrams, implementation guides, and other documentation developed in support of the engagement.

(D) All templates, terraform (IaC), scripts, source code, and other artifacts developed in support of the engagement.

(E) Project Closure report.

4.3. In Scope. The following systems, technologies and/or activities are within the scope of the Services:

(A) Design the landing Zone based on AWS best practices for Network, Security, Shared services, and workload Account.

(B) Design the Intelligent Devsecops platform using chain-off tools (open source) with an ability to handle the developer's workloads for CI/CD build, and automatic quality checks, notifications/alerts, Quality Dashboards & etc.

(C) Setup and run the Intelligent Devsecops platform using chain-off tools (Jenkins, SonarQube, Clair, selenium, JMeter, Nexus, Device Farm GIT, Container registry and AWS code commit for code commit.

(D) Implement the approved Landing zone design during the design phase.

(E) Implement high Level Security and Compliance design according to customer standards.

(F) Landing Zone Verification and deployment.

(G) perform Well architected review (WAR) of the Landing Zone and provide report.

(H) Enterprise Datalake:

a) Movement of 1973 tables from GATI & ACL data centres to AWS S3 using AWS DMS
b) CDC implementation for capturing changes from respective source data center and replicating the same in the Data Lake
c) CDC implementation for capturing changes from the S3 and replicating the same in staging layer of the source data centres.
d) Manage Data Catalog using AWS Glue Data Catalog & Crawlers

4.4. Out of Scope. Any systems, technologies and/or activities outside of the scope of Services in Section 4.3 are not included in the Services. Any change to the scope of the Services is subject to the Change Control Procedure. In particular, the following are outside the scope of the Services:

(A) Application-level issues and changes.

(B) Any application deployment.

(C) Any 3rd party Network and Firewall related changes.

(D) Migration services.

(E) Intrusion Prevention Service (IPS)

(F) Intrusion Detection Service (IDS)

(G) Data Processing or movement of data to any Data Warehouse

(H) Development of any dashboards is not part of this scope.

(I) Managing and collaborating of other customer projects outside of the project scoped in this document.

4.5. Project Duration. Based on requirements and assumptions set out in this SOW, the total estimated duration is Twelve (12) months. The current estimated project start date is End of October 2023, with estimated end-date on end of October 2024.This will be adjusted appropriately post engagement with customer as efficiencies or dependencies are better understood.

Project Phases	30-Oct Month 0	29-Nov Month 1	29-Dec Month 2	28-Jan Month 3	27-Feb Month 4	28-Mar Month 5	27-Apr Month 6	27-May Month 7	26-Jun Month 8	26-Jul Month 9	25-Aug Month 10	24-Sep Month 11	24-OCt Month 12	24-Nov Month 13
Mobilization and Kick Off														Managed Services
Landing Zone Design														
Devops Design				**										
GEMS Landing Zone & GEMS Devsecops Pipeline Implementation				**										
Devops Infra &SSO VPN & Dev Environment Build														
GEMS: SIT Environment Build														
GEMS: UAT Environment Build														
Warranty Support														
GEMS: Performance Testing														
GEMS: Production Environment Build														
Knowledge Transfer, Handover and Project Closure														

** Half weeks have been considered in this duration due to festivals and public holidays.

4.6. Staffing and Team Structure. Rackspace and Customer shall use reasonable efforts to allocate the following Rackspace Resources to meet the requirements of this SOW:

(A) Customer Resources.

Customer Role	Responsibilities
Customer Contact	• Serves as initial point of contact for Rackspace for duration of the SOW. • Provides feedback to ensure strategic objectives are properly communicated by Customer to the Rackspace team.

(B) Rackspace Resources.

Rackspace Role	Responsibilities
Project Manager	• Develop and manage the project plan/timeline. • Ensure due dates and deliverables are met. • Manage budget and facilitate billing. • Manage open items and issues log.

Rackspace Role	Responsibilities
	• Construct and document high-level plan with Rackspace and Customer. • Coordinate with project stakeholders to ensure barriers are removed. • Coordination of project meetings and workshops. • Will report directly to the Project Sponsor for project management-related duties, including team coordination, assignments, tasks, schedules, and project changes.
Solutions Architect	• Have relevant platform solution architecture and certification (as determined by Rackspace). • Have relevant experience with designing infrastructure for the relevant platform. • Have relevant experience with platform services. • Participate in workshops with the Customer's infrastructure and application engineers to understand application infrastructure requirements. • Responsible for producing high level design for Target Environment.
Cloud Engineer	• Have relevant architecture and infrastructure experience and be certified on the platform (as determined by Rackspace). • Have relevant experience automating infrastructure builds. • Deliver technical cloud platform activities as set out in the in-scope activities. • Performs deployment of infrastructure in accordance with approved designs • Participate in workshops with the Customer's infrastructure and application engineers to understand application infrastructure requirements
Rackspace Vendor: Data Architect	• Oversees the management and maintenance of the cloud computing system. • Responsible for developing cloud strategies, evaluating cloud applications and hardware, and organizing cloud systems to meet the operational needs of the customer with industry standard best practices.
Rackspace Vendor: Data Engineer	• Develop, constructs, tests & maintain complete architecture including ingestion layer, raw and curated zones, setting up and maintaining the end-to-end ETL pipeline using cloud services.
Rackspace Vendor: Project Manager	• Accountable for the overall success of the project and acts as a technical Project Management throughout the engagement. • Duties include Maintain a deliverable backlog, run the daily / weekly cadence, and manage overall deliverables.

5. ADDITIONAL ASSUMPTIONS. In addition to the assumptions in the Agreement, the Services, estimated timescales, and Fees are based on and subject to the following assumptions (and are subject to change if the assumptions are incorrect):

5.1. Customer provides full administrative access to in-scope environment and Account.

5.2. Unless expressly stated to the contrary in this SOW, attendance at Customer premises is not required and Services shall be delivered by Rackspace remotely.

5.3. The Services, estimated timescales and Fees are based on and subject to the following assumptions (and are subject to change if the assumptions are incorrect):

5.4. Upon completion of the deployment of the Landing Zone and the implementation of GEMS application (Dev & SIT Environment), the customer will provide sign off to Rackspace for the mobilize phase.

5.5. Customers retain overall responsibility for any business process impact and any process change implementations.

5.6. Unless conspicuously stated otherwise, Rackspace may utilize its Representatives to deliver all or part of the Services.

5.7. The estimated fees expected staffing and skill levels required for this SOW are based on available information provided by Customer to Rackspace; if additional time or personnel are deemed necessary due to a change in scope of assumptions, or work stoppage or delay resulting from Customer's action or inaction, adjustment to the fees and duration of this SOW may be necessary, subject to Rackspace's change management Procedure in Section 8 of PS terms.

5.8. Technical acceptance tests are conducted by Customer, or their nominated third party.

5.9. Rackspace is not required to perform any business application development in connection with their Services.

5.10. Customer is liable for all third-party tools license cost.

5.11. Project activities will be completed during Business Hours with the exception of any DNS which are expected to complete outside of normal Business Hours.

5.12. Customer applications have no known issues and will not require Rackspace engineering assist when migrating into the new environment.

5.13. Project delivery will not be delayed or impacted by any ongoing projects within the Customer's organization.

6. ADDITIONAL CUSTOMER RESPONSIBILITIES. In addition to the responsibilities in the Agreement, Customer shall:

6.1. Appoint a named Customer technical contact (having familiarity with Customer's information technology systems, and sufficient skill and knowledge in the technical aspects of the Services), and Customer project manager, to work with Rackspace for the duration of the Services.

6.2. Enable any required downtime for Service delivery (including liaising with end-user stakeholders and third parties to arrange maintenance windows, as may be necessary).

6.3. Perform user acceptance testing, migration execution steps, and remediation or changes required to applications (including due to hard coded IP addresses/names) as soon as is possible. Work in good faith to support Service delivery including: providing timely and appropriate access to Customer resources (including the Customer Configuration, accurate and complete information requested by Rackspace, technical assistance, personnel, materials, facilities, workspace, systems, technology and internet as may be applicable) as necessary; managing the Customer's own change control systems; and liaising with any end-user stakeholders and third parties (including incumbent providers) as may be reasonably requested. Customer remains responsible for all third-party charges incurred in the provision of Customer resources under this Section 6.4.

6.4. Appoint a representative that shall serve as a single point of contact for Rackspace for duration of the Services and shall provide feedback to ensure strategic objectives are properly communicated by Customer to the Rackspace team.

6.5. Remain responsible for the content and security of Customer Data, and selection and implementation of controls on Customer's access and use of Customer Data. Notwithstanding the foregoing, Rackspace Representatives shall abide by the security standards and procedures of Customer at all times at no additional cost to Rackspace.

6.6. Ensure that it has appropriate backup, security, and virus-checking procedures in place for any information technology systems provided by Customer or which may be affected by the Services to ensure that any Customer Data remains secure and is speedily and economically retrievable and shall ensure that Customer Data is backed up prior to commencement of the Services.

6.7. Not unreasonably withhold, delay, or condition any agreement, approval, consent, or similar action required for provision of the Services.

6.8. Requirements from customer for data lake development:

Deliverable type	Specifics	IT dependency	Infra requirements
AWS Infra setup (GATI + ACL)	Security Setup	Network team support to setup private network	
	Governance setup		AWS account access setup
	Establish connections with source systems	Network team to whitelist network*	Credentials & access required for all data sources
	Data migration infosec rules	Regional/country level rules & laws applicable for data migration	
	GATI data centres: Migration of historical data from various input sources (Approximate size of 600 GB)	Limitations/bottlenecks in network bandwidth for data transfer, system capacity	Documentation and walkthrough of all data sources (if any)
	ACL data centres: Migration of historical data from various input sources (Approximate size of 600 GB)	Limitations/bottlenecks in network bandwidth for data transfer, system capacity	Documentation and walkthrough of all data sources (if any)

6.9. Whitelisting of the IPs and establishing the private network with all data sources will be required to kick off the project for all data centres.

6.10. Support from AllCargo team:

(i) Network team – To configure VPN connection between AWS account and on prem network.

(ii) Database team – To configure the DMS prerequisite settings.

(iii) Back-up for historical data movement

(iv) CDC/Replication enablement

(v) Database User creation for data movement

6.11. Provide administrative access to existing AWS account(s).

6.12. Provide input for Network Services to be applied, included in Detailed design document.

(A) Suitable IP ranges

(B) WAF configurations including SSL certificates.

(C) Customer side VPN Configuration.

7. FEES & EXPENSES.

7.1. Fees. Unless expressly stated to the contrary in this SOW or modified by the Change Control Procedure, all Fees for the Services are fixed. Services shall be invoiced following completion of the milestones set out below and Customer acceptance of Deliverables (if applicable) in accordance with the Agreement or upon earlier termination. All fees are in USD and exclude GST.

Milestone	**Descriptions**	**Deliverable**	**Fee**
MS 1	SOW Execution	Signed SOW	$ 5,575.00
MS 2	Discovery and Landing Zone Design	Completion of Discovery and landing Zone design.	$ 27,875.00
MS 3	Enterprise Datalake: Design, Build and Migration.	Completion of Enterprise Datalake Design, build and Migration.	$ 33,450.00
MS 4	Infrastructure: Landing Zone & Devsecops Pipeline implementation.	Completion of Landing Zone & Devsecops Pipeline implementation.	$ 39,025.00
MS 5	Handover Project Closure	Completion of Knowledge transfer and handover Project Closure Report	$ 5,575.00
Total Fee			**USD$ 111,500**
Provisional Funding from AWS *(Refer to 7.3)*			**USD$ (111,500)**
Estimated Cost to Customer			**USD$ 0**

Table 1: Fee Schedule

7.2. Expenses. Travel and related expenses are included in the Fees set out in Section 7.1.

7.3. Third Party Funding. Amazon Web Services (AWS) has provisionally agreed to provide funding towards the Services under this SOW as per Clause 7.1. Third party funding is subject to final approval from such third-party funder. Customer is required to complete, sign, and return all necessary documentation (including project closeout documents) related to the third-party funding promptly and in any case within five Business Days of receipt in order to be granted any third-party funding. Customer remains solely responsible for securing third party funding and payment of all amounts due under this SOW, including payment of the third party funded amount in the event it is not approved by the third party or expires.

8. SOW CONTACTS.

The following SOW contacts may be replaced by the parties from time to time:

	Rackspace SOW Contact
Name	Bhuvnesh Soni
Title	Enterprise Sales India
Email	bhuvnesh.soni@rackspace.com
Telephone	+91 98866 60518

9. APPENDIX.

9.1. High Level Architectures.

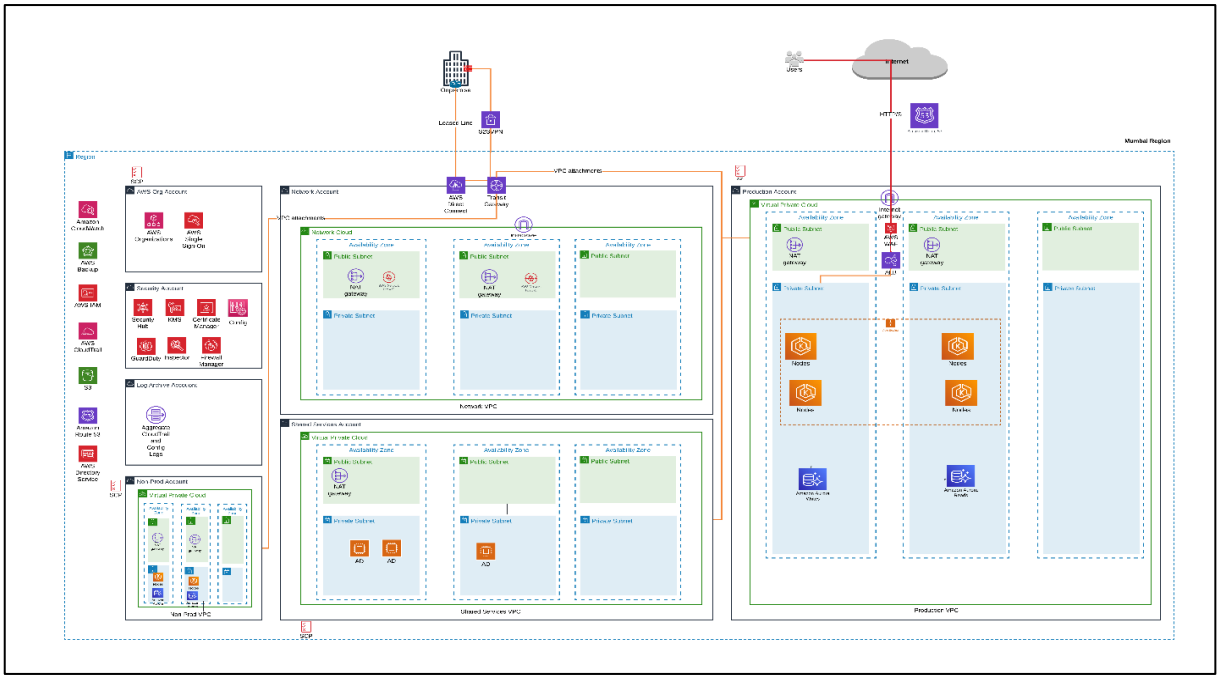

Figure 1: GEMS Landing Zone

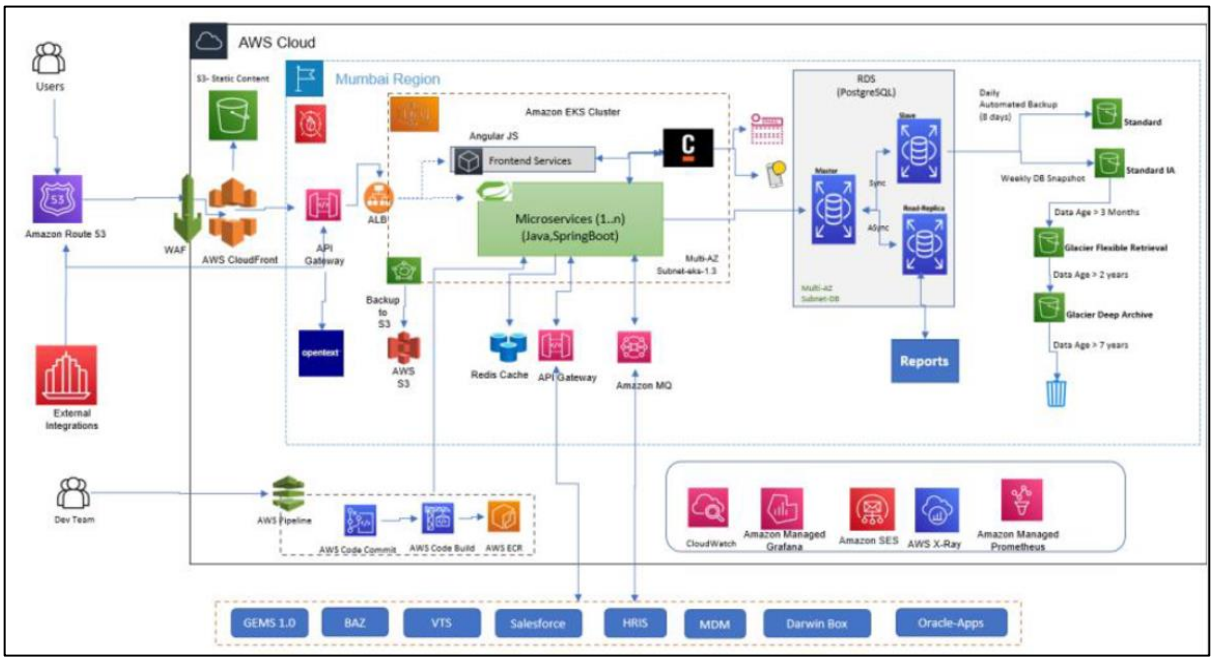

Figure 2: DEVSECOPS Architecture

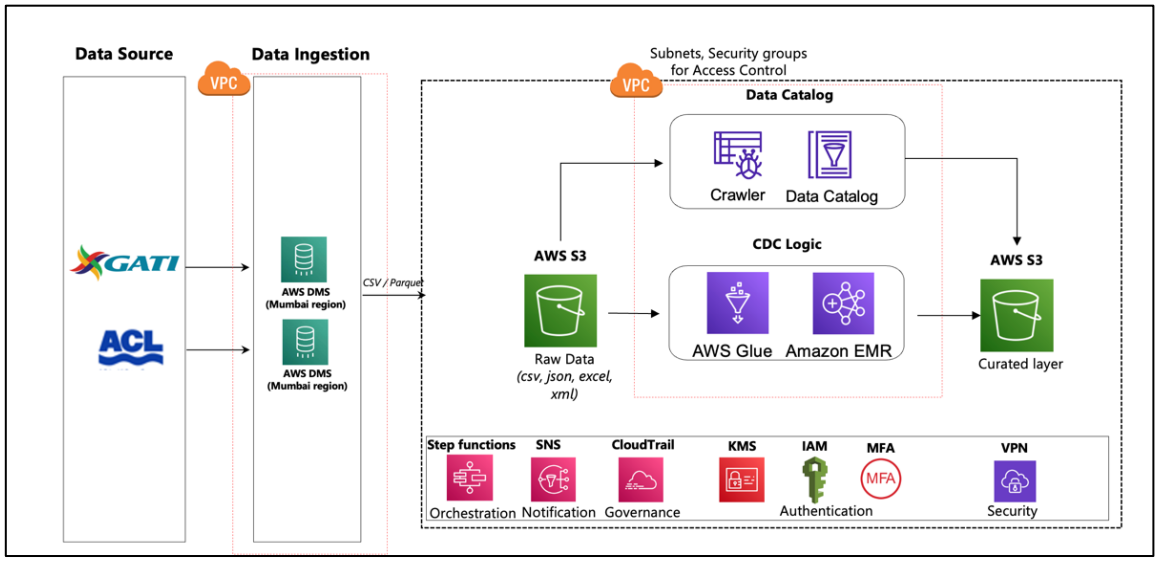

Figure 3: Datalake Architecture