Government eProcurement System

eProcurement System Government of India

Tender Details

Date : 27-Sep-2022 11:58 AM

🖶 Print

Basic Details

Organisation Chain	Government e-Marketplace (GeM)
Tender Reference Number	GeM/Hiring_Of_MSP/2022/01
Tender ID	2022_GeM_714702_1

Tender Type	Open Tender	**Form of contract**	QCBS
Tender Category	Services	**No. of Covers**	4
General Technical Evaluation Allowed	Yes	**ItemWise Technical Evaluation Allowed**	No
Payment Mode	Offline	**Is Multi Currency Allowed For BOQ**	No
Is Multi Currency Allowed For Fee	No	**Allow Two Stage Bidding**	No

Payment Instruments

Offline	S.No	Instrument Type
	1	Bank Guarantee

Cover Details, No. Of Covers - 4

Cover No	Cover	Document Type	Description
1	Fee	.pdf	Fee related documents
2	PreQual	.pdf	Pre qualification criteria related documents
3	Technical	.pdf	Technical criteria related documents
		.pdf	Additional documents (if any)
4	Finance	.xls	Financial bid related documents

Tender Fee Details, [Total Fee in ₹ * - 0.00]

Tender Fee in ₹	0.00		
Fee Payable To	Nil	**Fee Payable At**	Nil
Tender Fee Exemption Allowed	No		

EMD Fee Details

EMD Amount in ₹	1,50,00,000	**EMD through BG/ST or EMD Exemption Allowed**	Yes
EMD Fee Type	fixed	**EMD Percentage**	NA
EMD Payable To	Government e Marketplace	**EMD Payable At**	New Delhi

Click to view modification history

Work /Item(s)

Title	RFP
Work Description	REQUEST FOR PROPOSAL Selection of Managed Service Provider for Design, Development, Implementation, Operation and Maintenance of Government e-Marketplace
Pre Qualification Details	As per RFP
	N/A

Independent External Monitor/Remarks					
Show Tender Value in Public Domain	No				
Tender Value in ₹	12,00,00,00,000	Product Category	Info. Tech. Services	Sub category	Hiring of MSP
Contract Type	Tender	Bid Validity(Days)	120	Period Of Work (Days)	2000
Location	New Delhi	Pincode	110001	Pre Bid Meeting Place	As per RFP
Pre Bid Meeting Address	As per RFP	Pre Bid Meeting Date	19-Oct-2022 11:00 AM	Bid Opening Place	New Delhi
Should Allow NDA Tender	No	Allow Preferential Bidder	No		

Critical Dates

Publish Date	27-Sep-2022 03:00 PM	Bid Opening Date	16-Nov-2022 03:00 PM
Document Download / Sale Start Date	27-Sep-2022 03:00 PM	Document Download / Sale End Date	15-Nov-2022 03:00 PM
Clarification Start Date	27-Sep-2022 03:00 PM	Clarification End Date	19-Oct-2022 11:00 AM
Bid Submission Start Date	27-Sep-2022 03:00 PM	Bid Submission End Date	15-Nov-2022 03:00 PM

Tender Documents

NIT Document	S.No	Document Name	Description	Document Size (in KB)
	1	Tendernotice_1.pdf	RFP	10766.68

Work Item Documents	S.No	Document Type	Document Name	Description	Document Size (in KB)
	1	BOQ	BOQ_751872.xls	BOQ	237.50
	2	Tender Documents	RFPMerged.pdf	RFP	10752.86

View GTE /QCBS Details

S.No	Particulars	Expected Value	Mandatory	Points (Weightage)
1.0	Normalized final Technical Score as per RFP	Yes	Yes	100

Bid Openers List

S.No	Bid Opener Login Id	Bid Opener Name	Certificate Name
1.	director-amitk@gem.gov.in	Amit Kumar Agrawal	AMIT KUMAR AGRAWAL
2.	director-gem@gem.gov.in	Anuj Kumar	Anuj Kumar
3.	director-akm@gem.gov.in	Anand Kumar Mishra	ANAND KUMAR MISHRA

GeMARPTS Details

GeMARPTS ID	CJ5T4P2RRVK1
Description	Hiring of MSP
Report Initiated On	27-Sep-2022
Valid Until	27-Oct-2022

Tender Properties

Auto Tendering Process allowed	No	Show Technical bid status	Yes
Show Finance bid status	Yes	Show Bids Details	Yes
BoQ Comparative Chart model	Normal	BoQ Compartive chart decimal places	4

BoQ Comparative Chart Rank Type	L	Form Based BoQ	No

Tender Inviting Authority

Name	CEO-GeM
Address	CEO-GeM

Tender Creator Details

Created By	Anuj Kumar
Designation	Director Administration
Created Date	27-Sep-2022 11:30 AM

GOVERNMENT OF INDIA
MINISTRY OF COMMERCE & INDUSTRY

Government e-Marketplace

3rd floor, Tower II, Jeevan Bharti Building, Janpath, Connaught Place,
New Delhi-110001

REQUEST FOR PROPOSAL

Selection of Managed Service Provider (MSP) for Design, Development, Implementation, Operation & Maintenance of Government e-Marketplace (GeM)

RFP Number: GeM/Hiring_Of_MSP/2022/01

Volume-1: Terms of Reference

Document Control

Date	Version	Description

Contents

List of Tables

List of Figures

ACRONYMS

Abbreviation	Description
ABAC	Attribute-based access control
ACASH	Association of Corporations and Apex Societies of Handlooms
ACD	Automatic Call Distributor
ACEOs	Additional Chief Executive Officer
ADM	Application Data Management
AES	Advanced Encryption Standard
AHT	Average Handing Time
AI	Artificial Intelligence
AIX	Advanced Interactive Executive
AMC	Annual Maintenance Contract
ANI	Automated Number Identification
ANN	Artificial neural networks
API	Application Programming Interface
ASP	Active Server Pages
ATCs	Additional Terms and Conditions
AV	Anti-Virus
AWS	Amazon Web Services
B.E	Bachelors in Engineering
B.Tech	Bachelors in Technology
BAU	Business Administration Unit
BCA	Bachelors of Computer Application
BCP	Business Continuity Planning
BG	Bank Guarantee
BHEL	Bharat Heavy Electricals Limited
BI	Business Intelligence
BIS	Business Intelligence Systems
BOQ	Bill of Quantity

BP	Bidding Parameter
BPM	Business Process Management
BPMN	Business Process Modeling Notation
BQM	Bottom Quartile Management
BRD	Business Requirement Document
BSU	Business Services Unit
CA	Chartered Accountants
CAB	Change Advisory Board
CAG	Comptroller and Auditor General of India
CAGR	Cumulative Annual Growth rate
CBIC	Central Board of Indirect Taxes & Customs
CBO	Chief Buyer Officer
CBT	Computer Based Training
CC	Common criteria
CCA	Controller of Certifying Authorities
CDR	Call Detail Record
CEO	Chief Executive Office
CERTIN	Indian Computer Emergency Response Team
CFO	Chief Finance Officer
CGA	Comptroller General of Accounts
CGDA	Controller General of Defence Accounts
CHRO	Chief Human Resource Officer
CI-CD	Continuous Integration, Continuous deployment
CIDR	Classless Inter-Domain Routing
CIN	Corporate Identification Number
CIO	Chief Information Officer
CIPS	Chartered Institute for Procurement and supplies
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CLI	Command Line Interface

CMC	Comprehensive Maintenance Contract
CMMi	Capability Maturity Model Integration
CMS	Catalogue Management System
CO	Commanding Officer
COBIT	Control Objectives for Information and Related Technologies
COTS	Commercial-Off-The-Shelf
CPPP	Central Public Procurement Portal
CPSEs	Central Public Sector Enterprises
CPSU	Central Public Sector Undertakings
CPU	Central processing utilization
CQRS	Command Query Responsibility Segregation
CR.	Crores
CRAC	Consignee Receipt & Acceptance Certificate
CRI-O	Container Runtime Interface (Open Container Initiative)
CRM	Customer Relationship Management
CRMC	Change request management committee
CRN	Change request Number
CRPF	Central Reserve Police Force
CRs	Change Requests
CSAT	Customer Satisfaction
CSE	Computer Science Engineering
CSL	Critical Service Level
CSP	Cloud Service Provider
CSS	Cascading Style Sheets
CTI	Computer Telephony Integration
CTO	Chief Technology Officer
CV	Curriculum Vitae
CVC	Central Vigilance Commission
DA	Demand Aggregation
DAM	Database Activity Monitoring

DAO	Data Access Objects
DB	Data base
DC	Data Center
DCEOs	Deputy Chief Executive Officers
DDO	Drawing and Disbursement Officer
DDOS	Distributed Denial-of-Service
DDR	Double Data Rate
DeitY	Department of Electronics and Information Technology
DES	Data Encryption Standard
DGQA	Directorate General of Quality Assurance
DHCP	Dynamic Host Configuration Protocol
DIPP	Department of Industrial Policy and Promotion
DLP	Data Loss Protection
DMAIC	Define, Measure, Analyze, Improve, Control
DMZ	Demilitarized zone
DNIS	Dialed Number Identification Sequence
DNS	Domain Name System
DoT	Department of Telecommunications
DP	Delivery Period
DR	Disaster Recovery
DRDO	Defence Research and Development Organization
DSAT	Digital Supervisory Audio Tones
DSC	Digital Signature Certificate
DSR	Daily Status Report
DTO	Data Transfer Objects
DWT	Data Warehouse Testing
EA	Enterprise Architecture
eBG	electronic Bank Guarantee
eGS	e-GramSWARAJ
eGSPI	eGramSwaraj PFMS Interface

EIL	Engineers India Limited
EMD	Earnest Money Deposit
EMS	Element Management System
EoDB	Ease of doing business
e-PBG	electronic Performance Bank Guarantee
ERP	Enterprise Resource Planning
ESM	Emergency Security Management
ETL	Extract Transform Load
FA	Forward Auction
FAQ	Frequent Asked Questions
FCR	First Contact resolution
FCRA	Foreign Contribution (Regulation) Act
FLLP	Foreign Limited Liability Partnership
FRS	Functional Requirement Specification
FSSAI	Food Safety and Standards Authority of India
FTD	For the date
FTE	Full Time Employee
FTP	File Transfer Protocol
FTR	First Time Resolution
FY	Financial Year
GAR	GeM Availability Report
GB	Gigabyte
GCC	Government Community Cloud
GCP	Google Cloud Platform
GDCC	Government desktop core configuration
GeM	Government e-Marketplace
GFR	General Financial Rules
GMV	Gross Merchandize Value
GPA	GeM Pool Account
GSM	Global System for Mobile communication

GST	Goods and service Tax
GSTIN	Goods and Service Tax Identification Number
GSTN	Goods and service Tax Network
GUR	GeM Utilization Ratio
HA	High Availability
HIDS	Host-based intrusion detection system
HLD	High-level Design
HOD	Head of Department
HR	Human Resource
HSN	Harmonized System of Nomenclature
HTML	Hyper Text Markup Language
HTTPS	Hyper Text Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IBM	International Business Machines Corporation
ICT	Installation commissioning and testing feature
ID	Identity Document
IDS/IDP	Intrusion Detection and Prevention
IEC	International Electrotechnical Commission
IFMS	Integrated Financial Management System
IFSC	Indian Financial System Code
IIS	Internet Information Services
IM	Incident Management
iMMS	Integrated Material Management System
IndEA	India Enterprise Architecture
INR	Indian Rupee
IOCL	Indian Oil Corporation Limited
IOPS	Input/Output operations per second
iOS	iPhone Operating System
IP	Internet Protocol

IPAS	Integrated Payroll and Accounting System
IPSec	Internet Protocol Security
IRePS	Indian Railways Electronic Procurement System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information technology
ITC	Input tax credit
ITC-HS	Indian Trade Classification- Harmonized System
ITD	Income Tax department
ITIL	Information technology Infrastructure Library
ITOPS	IT related operational reports
ITR	Income tax return
ITSM	Information Technology Service Management
ITSRA	Insider Threat Security Reference Architecture
IVR	Interactive Voice Response
IVRS	Interactive Voice Response System
JBOSS	Java Beans Open Source Software
JD	Job description
JMS	Java Message Service
JSON	JavaScript Object Notation
JWT	JSON Web Token
KB	Knowledge Base
KNE	Knowledge Navigation Experts
KPI	Key Performance Indicators
KT	Knowledge Transfer
KVIC	Khadi and Village Industries Commission
KYC	Know your Customer
LAN	Local Area Network
LCS	Least Cost Selection
LD	Liquidated Damages

LDAP	Lightweight Directory Access Protocol
LLB	Bachelor of Law
LLD	Low-level Design
LMS	Learning Management System
LoV	List of values
LXC	Linux Containers
LXD	Linux Container Hypervisor
M.E	Masters in Engineering
M.Tech	Masters in Technology
MB	Megabytes
MBA	Master in Business Administration
MCA	Masters in Computer Application
MCA-21	Ministry of Corporate Affairs
MD	Managing Director
MDM	Master data Management
MeiTY	Ministry of Electronics and Information Technology
MII	Make in India
MIS	Management Information Systems
MKP	Marketplace Portal
ML	Machine Learning
MoPR	Ministry of Panchayati Raj
MOPS	Multi Option Payment System
MPLS	Multiprotocol Label Switching
MRP	Maximum Retail Price
MS	Microsoft
MSDG	Mobile Service Delivery Gateway
MSEs	Micro and Small Enterprises
MSMEs	Micro Small and Medium Enterprises
MSP	Managed Service Provider
MTD	Month to date

NAC	Network Access Control
NBFC	Non-Banking Financial C
NCR	National Capital Region
NEFT	National Electronic Fund Transfer
NeGP	National e-Governance Plan
NFS	Network File Systems
NGINX	Engine X
NIC	National Informatics Center
NIDS	Network Based Intrusion Detection System
NIST	National Institute of Standards and Technology
NITRA	Northern India Textile Research Association
NLP	Natural language processing
NPAE	Non-PFMS Agencies/Facilities
NSDG	National e-Governance Service Delivery Gateway
NSDL	National Security Depository Limited
NSIC	National Small Industries Corporation
O&M	Operations & Maintenance
OBIEE	Oracle Business Intelligence Suite Enterprise Edition
OCP	OpenShift Container Platform
OEM	Original Equipment Manufacturer
OEM TM	Original Equipment Manufacturer Trademark
OLAP	Online analytical processing
OLTP	Online transaction processing
OM	Office Memorandum
ONDC	Open Network for Digital Commerce
ONGC	Oil and Natural Gas Corporation
OS	Operating System
OSP	Original Service Provider
OTP	One time Password
PAC	Proprietary Article Certificate

PAN	Permanent Account Number
PAO	Pay Account Office
PBG	Performance Bank Guarantee
PC	Personal Computer
PCI	Peripheral Component Interconnect
PD	Project Director
PDF	Portable Document Format
PERL	Practical Extraction and Report Language
PFMS	Public Financial Management System
PHP	Hypertext Preprocessor
PIFI	Personally Identifiable financial Information
PII	Personally Identifiable Information
PIU	Project Implementation Unit
PKCE	Proof Key for Code Exchange
PKI	Public Key Infrastructure
PMU	Project Management Unit
POP	Point Of Presence
PPT	Power point
PRC	Provisional Receipt Certificate
PRI	Primary Rate Interface
PS	Primary Support
PSUs	Public Sector Units
PVC	Price Variation Clause
QA	Quality Assurance
QCBS	Quality-Cost-Based Selection
QCI	Quality Council of India
RA	Reverse Auction
RACI	Responsible, Accountable, Consulted and Informed
RADIUS	Remote Authentication Dial-In User Service
RAG	Red-Amber-Green

RAID	Risk, Assumptions, Issues and Dependencies
RAM	Random Access Memory
RBAC	Role-based access control
RBI	Reserve Bank of India
RCA	Root Cause Analysis
RDBMS	Relational Database Management System
REST API	Representational State Transfer API
RFC	Request for Comment
RFP	Request for Proposal
RMS	Request Management System
RPO	Recovery Point Object
RTGS	Real Time Gross Settlement
RTO	Recovery Time Object
RXIL	Receivables Exchange of India Limited
SAIL	Steel Authority of India Limited
SBI	State Bank of India
SCN	Show Cause Notice
SDAC	Service Delivery and Acceptance Certificate
SDK	Software Development Kit
SDLC	System Development Life Cycle
SELO	Service & Loyalty
SEM	Security event Management
SEO	Search Engine Optimization
SHG	Self Help Group
SI	System Integration
SIAM	Service Management
SIEM	Security Information and event Management
SIM	Security Information Management
SIP	Service Improvement Plan
SL	Service Learning

SLA	Service Level Agreement
SMB	Server Message Block
SME	Subject matter Expert
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	System and Organization Controls
SOP	Statement of
SPA	Single Page Applications
SPOC	Single Point of contact
SPV	Special Purpose Vehicle
SQL	Structured Query Language
SRM	Security reference model
SRS	Software Requirement Specification
SS	Secondary Support
SSD	Solid state drive
SSDG	State e-Governance Service Delivery Gateway
SSL	Secure Socket Layer
SSL VPN	Secured Socket Layer Virtual Private Network
SSO	Single Sign on
STQC	Standardisation Testing and Quality Certification
SVC	Statutory Variation Clause
TAN	Tax Deduction Account Number
TAT	Turnaround Time
TB	Terabyte
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

TDS	Tax deduction at Source
TER	Technical Evaluation Report
TLS	Transport Layer Security
TMO	Transformation Management Office
TNA	Training Need Analysis
TOGAF	The Open Group Architecture Framework
TP	Technical Parameters
TPA	Third-Party Auditors
TPS	Transaction per second
TRAI	Telecom Regulatory Authority of India
TReDS	Trade Receivables electronic Discounting System
TRIFED	Tribal Cooperative Marketing Development Federation of India Limited
TSU	Technical Services Unit
UAM	Udyog Aadhaar Memorandum
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UI	User Interface
UIDAI	Unique Identification Authority of India
UNIX	Uniplexed Information Computing System
UNSPSC	United Nations Standard Products and Service Code
URL	Uniform Resource Locator
USB	Universal Serial Bus
UX	User Experience
VA	Vendor Assessment
VAE	Vendor Assessment Exemption
VAPT	Vulnerability assessment and Penetration testing
vCPU	Virtual CPU
VI	Visual
VLAN	Virtual Local Area Network
VM	Virtual Machine

VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
vRam	Video RAM
WAF	Web Application Firewall
WAN	Wide Area Network
WBS	Work Breakdown Structure
WEP	Wired equivalent privacy
WORM	Write once, Read Many
WPA	Wi-fi Protected Access
WS	Web Services
XML	Extensible Markup Language
XSS	Cross site Scripting

1. Introduction

1.1 About GeM

Government e-Marketplace (GeM) is the National Public Procurement Portal for procurement of goods and services for all Central Government and State Government Ministries, Departments, Public Sector Units (PSUs) and affiliated bodies. The GeM initiative was launched on August 9, 2016, by the Ministry of Commerce and Industry, Government of India, and a Special Purpose Vehicle (SPV) by the name of Government e-Marketplace (GeM) was set up as the National Public Procurement Portal on 17th May 2017 in pursuance of the approval of the Union Cabinet accorded on 12th April 2017. GeM was incorporated as a 100% Government owned not-for-profit Private Limited Company, registered under Section 8 of the Companies Act, 2013.

The primary purpose of GeM is to increase transparency, efficiency, and inclusivity of public procurement by eliminating Buyer-Supplier interface and moving to an end-to-end, online solution. It acts as a centralized and unified public procurement platform for government Buyer organizations and suppliers of goods and services, accompanied by:

1. Policy reforms for current processes of public procurement ecosystem

2. Driving Inclusiveness and Ease of Doing Business (EoDB) with the government (especially for smaller organizations such as MSMEs)

3. Standardization of processes backed by the regulatory framework

4. A fully automated system enabled through world-class technologies

GeM is a major transformational initiative ushering in a paradigm shift in the way Government has been managing its procurement function hitherto and has already been a recipient of multiple awards and accolades. For instance, Chartered Institute for Procurement and Supply (CIPS) has awarded GeM as the winner under the 'Best use of digital technology' category at its Excellence in Procurement awards, 2021. GeM was also named the winner of the Dun & Bradstreet India's Top PSUs Awards, 2021 in the category of "E-Governance Solutions for Public Procurement."

1.2 Existing system overview

GeM has transformed legacy procurement systems through a disruptive marketplace model and the use of technology, analytics, and digitization of processes. It has made significant strides since its inception, as depicted below:

Financial year (FY)	Total Actual GMV (INR CR.)
FY 16-17	422
FY 17-18	6,188
FY 18-19	17,462
FY 19-20	22,991
FY 20-21	38,580
FY 21-22	1,06,647

Table 1: GeM GMV

1. More than 200% Cumulative Annual Growth Rate (CAGR) from FY2016-17 to FY2021-22

2. Approx. 33.2 Lakh number of orders or transactions in FY2021-22

3. Approx. INR 45,500 Cr. procurement in FY2021-22 from Central PSUs on GeM, with more than 500% YoY growth with respect to FY2020-21

4. Approx. 15%+ and 180%+ growth in Buyers & Sellers onboarding compared to FY2020-21

GeM has enabled an online, end-to-end marketplace for procurement of goods and services based on its three founding principles or pillars, viz., transparency, efficiency, and inclusivity.

Transparency: GeM constantly engages with procuring entities and the Department of Expenditure for rolling out different functionalities and making the public procurement process more transparent. Several features have been deployed to make the procurement process completely contactless and faceless, including but not limited to:

1. Rich listing of products and services across several categories to Buyers for easy browsing and appreciation of the marketplace.

2. Quicker procurement cycle and automated processes for enforcement of compliance.

3. Better price discovery and increased competition during the Bidding Process.

4. Continuous, transparent, and robust vendor rating system to safeguard Buyer interest.

5. No barrier to entry and no fees for registration, brand approval and product uploads.

6. Increased transparency by making reasons for rejection visible to all Sellers.

5. Faster and easier payment gateways for quick payment - integration with Banks / TReDS / ERP Systems to facilitate timely payments and bill discounting.

6. AI-ML investments such as NLP-based search engine and AI-based chatbot support.

7. Forward auction module to facilitate government auctions for assets and monitor the complete selling life cycle of their assets.

GeM is looking to further invest heavily in advanced analytics tools to not only flag inappropriate buying behavioral patterns of Buyers and Sellers but also proactively guide and help them in appropriate decision making.

Efficiency: An independent study by the World Bank[1] indicated substantial savings due to GeM's ability to pool in more participation. In other procurement portals in India, the average number of bids per tender hovered around 3 to 4 bids while an average value of 7-9 bids per tender was observed in GeM. This has also attracted international media coverage and attention; for instance, a Bloomberg article[2] published in September 2020 projected GeM as the Indian government's own Amazon, having saved about $1 billion for the exchequer. Economic survey 2021-22, conducted by Department of Economic Affairs, also observed prices on the GeM portal on sample basis to be on an average 9.5% lower as compared to prices on other platforms for the sample set. As GeM grows and more and more public procurement is routed through GeM, the efficiency is bound to increase due to more transparency, visibility, and ease of doing business.

Inclusivity: Beyond its normal mandate of providing a Transparent and efficient public procurement, GeM has also taken responsibility for ensuring proper implementation of the MSE and MII policies of Govt. by enabling the use of technology to push proper clauses in the bids. In FY2021-22, approx. 55% of the total GeM GMV was awarded to MSEs, thus providing high online market access to under-served Seller groups and reinforcing the "Atmanirbhar Bharat", "Vocal for Local", and "Make in India (MII)" initiative under Government of India's policy to promote local MSEs. In the past GeM has launched various initiatives such as Womaniya, Saras Collection, TribesIndia eStore, Bamboo, Startup Runway, etc. for onboarding of artisans, weavers, startups, etc. To drive inclusivity further, GeM is integrating with Panchayati Raj Institutions to allow online buying and selling by the Panchayats at the grassroot level. The pilot in Gurgaon district panchayats has been successfully completed. GeM has also done integration with IndiaPost for extending logistics services at the grassroot level. Additionally, efforts are also being made to rehabilitate small business sector by improving financial access via GeM SAHAY. This initiative facilitates small Sellers to avail credit financing from various integrated Lenders for the orders received on GeM Portal.

Apart from these three pillars, GeM has also been instrumental in managing the Covid-19 pandemic through various initiatives such as an oxygen drive carried out during the Covid crisis to onboard suppliers of compressed medical oxygen gas cylinders on GeM. Currently GeM hosts 250 Covid-19 medical categories; over 4.73 Lakh orders have been placed through the same since March 2020.

---

[1] INDIA – A Study to Understand the Impact of Government e-Marketplace (GeM) on Procurement Performance Using Data Analytics, World Bank, June 2020
[2] https://www.bloomberg.com/news/articles/2020-09-18/government-s-version-of-amazon-com-helps-india-save-1-billion

2.   Format of this RFP

The content of this RFP has been detailed over a set of three volumes as explained below:

1. **Volume 1: Terms of reference including the scope of work for MSP, functional, non-functional and technical requirements, timelines, etc.**

   Volume 1 of this RFP includes the detailed scope of work for the MSP, functional, technical, and operational requirements of the intended solution and related annexure(s).

2. **Volume 2: Instruction to bidders for submission, and Bidding & Commercial Terms of this RFP**

   Volume 2 of this RFP includes instructions to the bidders for submission, details on the technical and commercial evaluation criteria and their related forms, formats, guidelines, and related annexure(s).

3. **Volume 3: Legal Terms & Master Service Agreements**

   Volume 3 of this RFP includes the draft Master Services Agreement and Service Level Agreement to be signed between GeM and the Managed Service Provider (MSP)

<u>Note:</u>

In this RFP, the term 'Purchaser' refers to Government e-Marketplace (GeM). GeM/ Purchaser have been interchangeably used throughout the RFP documents. The term 'Bidder' refers to an entity submitting a proposal as a response to this RFP. The term 'Managed Service Provider (MSP)' refers to the successful Bidder who is contracted for implementation of the GeM solution (also referred to as 'the Project'), per terms and conditions specified in this RFP and shall be deemed to include the MSP, its agents, successors, representatives, & permitted assigns.

3. Scope of Work

3.1 Implementation of GeM Solution

3.1.1 Overview

The Scope of Work for the MSP is to re-design, re-develop, re-implement, operate and maintain the new GeM platform. In addition, the MSP shall also understand current GeM platform, takeover in a phased manner and support operations and maintenance of current GeM platform till new platform Go-live. Broadly the Scope of Work for the MSP shall be as explained in following sections.

3.1.2 Application Design, Development, and Implementation

This track comprises the development of the new GeM platform and all the components as defined in Volume 1 Section 8.1 of this RFP with directional alignment to technical requirements specified in Volume 1 Section 8.2 of this RFP.

1. MSP's scope of work shall include the implementation of a platform that would include all customizations and configurations to handle end to end workflow as listed in this RFP. The platform shall support multiple languages and bi-lingual (English, Hindi) search capability as mentioned in Volume 1 Section 8.2.9 of the RFP.

2. While doing application development and maintenance the MSP is expected to follow and comply with the processes as per CMMi Level 5 standards.

3. The MSP shall create the GeM Mobile App (both for Android and iOS latest version) with following functionalities:

   a. Reporting features such as key metrics, dashboards, etc. as per alignment with GeM during the design phase as mentioned in Volume 1 Section 5 of this RFP.

   b. Real-time alerts & notifications against certain events such new bid created, progress milestones status, etc. (as aligned with GeM during design phase).

   c. Application notifications based authentication of the user for different purposes such as registration, login, bid creation, bid submission, etc. (as aligned with GeM during design phase).

4. MSP shall also develop a web app of the GeM Portal (apart from the mobile app) which can be accessed using smartphones/tablets.

5. MSP shall create online functionality for enabling the role of Certifying Authority for GeM to perform Aadhaar based e-KYC, electronic signature, and Digital Signing of documents /data.

MSP shall also provision for all infrastructural requirements for the same functionality, with physical separation via air gap, as per guidelines defined by Controller of Certifying Authorities.

6. Module for user management of procurement officials needs to be developed. Each Buyer (Ministry/Department/PSU/etc.) will manage its users through a nominated administrator(s) who will have limited admin rights over the user management module for creation, deletion, modification, or transfer, etc. of the users for the respective Ministry/Department/PSU/etc.

7. MSP to integrate the GeM Solution with different entities such as payment gateways, banks, UIDAI, GSTN & ITD, Credit rating agencies, Ministry of Corporate Affairs, CPSEs, PFMS, IFMS of States, Lending agencies, etc.

8. MSP would be responsible for identifying obsolete data on the current GeM platform and perform data archival as per the policy.

9. GeM will be the owner of the application software developed for this project including source code, all related documentation created for the project. MSP shall be responsible for maintaining proper documentation related to the project in a structured repository, with proper version control.

10. Each phase of application development and implementation for the GeM System needs to follow the below lifecycle:

3.1.2.1 Requirements Gathering

1. The MSP must perform a detailed assessment of the business and IT solution requirements as mentioned in this RFP. Additionally, the MSP is required to carry out exhaustive requirements gathering exercises with the GeM team, including but not limited to review of existing code, BRDs and other documentation, for understanding and drafting the requirements. While doing so, the MSP is expected to do at least the following: Translate all the requirements into detailed Business Requirements Document (BRD), Functional Requirement Specification (FRS) & Software Requirements Specification (SRS) Documents. This is required for any minor to major enhancements following standard templates.

2. Develop and follow standardized templates for capturing requirements and system documentation.

3. Maintain a traceability matrix from the SRS stage onwards for the entire implementation.

4. Obtain the required signoffs from user groups formed by the GeM.

While indicative functional details of the envisaged system are provided in Volume 1 Section 8.1 of this RFP, some of the processes and forms may change at the time of implementation. The MSP needs to consider this fact while submitting its proposal. No extra cost shall be paid for such changes till the completion of Go-Live of the new platform. All major changes post this for each phase shall be handled through the change control process. The Service provider shall as a starting point gather the requirements as specified in this RFP.

3.1.2.2 Analysis & Design

The MSP shall build the solution in compliance with the requirements outlined in this RFP. The MSP needs to comply with the Solution Architecture principles and other details mentioned in Volume 1 Section 8.2 of this RFP. However, the MSP is free to suggest a better /equivalent alternate architecture which will be subject to evaluation by GeM. The architectural, cloud and sizing guidelines mentioned in Volume 1 Section 8.2, 8.3, and 8.4 of the RFP respectively, are proposed guidelines that are directional in nature, and if required, can be modified with mutual agreement between GeM and MSP at any stage during the execution of Agreement.

3.1.2.3 API's Management and Usage

1. Data exchange between the GeM System and other Internal/ External Systems will be carried out preferably through APIs. The MSP, in consultation with the GeM, will also be required to set up a process for the issuance of standards for the GeM System APIs.

2. The MSP needs to set up, operationalize and maintain a system for APIs, indicative functionalities of which are included in Volume 1 Section 8.2 of this RFP.

3. The MSP shall be entirely responsible for proposing the solution which satisfies all features, functions and performance requirements as described in this RFP and relevant documents. The MSP shall be responsible for the design, development, implementation and maintenance of the proposed solution and shall ensure that the proposed system/application/product, are current level "N" (where N is the current latest commercially available release) at the cost of the MSP for the entire life of the project.

3.1.2.4 Overall Development, Commissioning, Configuration, and Implementation methodology

The MSP shall consider the scope of work, develop, commission, configure, and implement a solution that meets the GeM System's requirements. In the technical proposal, the MSP needs to elaborate on the proposed approach for software development, commissioning, configuration & implementation.

MSP shall use the agile/iterative methodology unless specifically requested by GeM to use the waterfall approach. MSP shall advise on the two methodologies and final decision in this regard will be taken by the GeM. Regardless of the methodology, a continuous delivery pipeline should be used to deliver the application. In the case of the agile methodology, the build and test phases shall involve

portions of the applications being worked upon in iterations and provided to GeM for testing and providing feedback. This project development methodology is represented in the diagram below (can be modified according to GeM and MSP's agreement). Continuous GeM involvement is recommended to ensure that any concerns and issues are caught early in the Software Development Lifecycle.
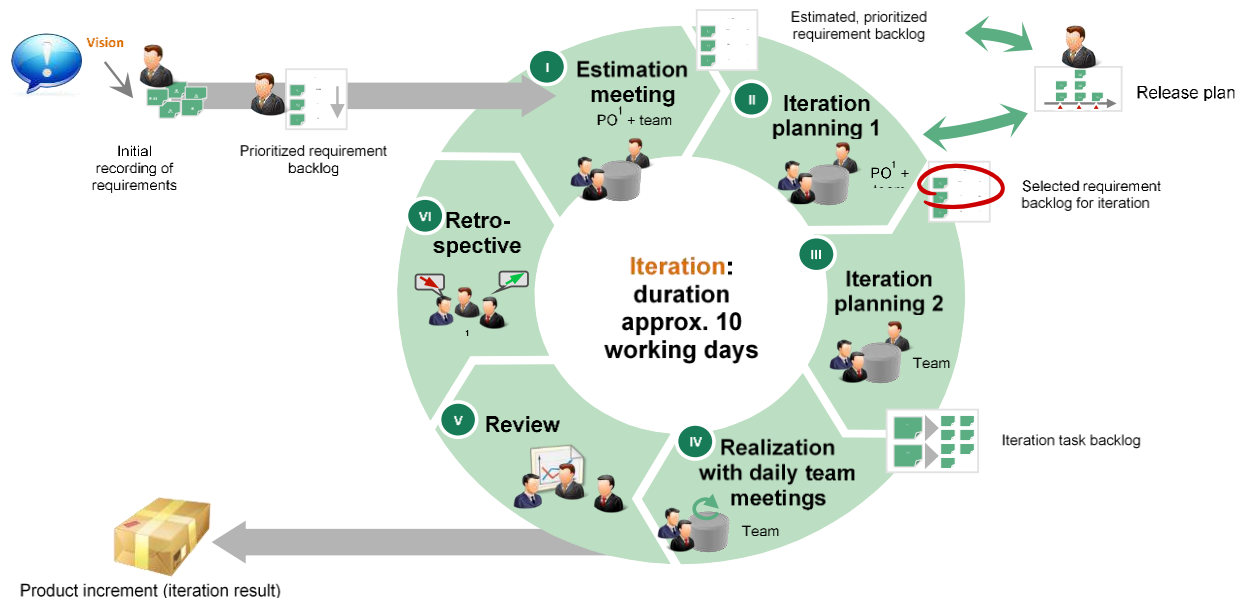
Figure 1: Ideal Software Development Lifecycle

3.1.2.5 Application Requirements Specifications & Business Analysis

1. Application Requirements Definition Services are the activities associated with the definition of process standards (e.g., coding standards, naming convention, user interface standards, interfaces standards etc.), develop processes and procedures to meet applications standards and other technology standards and assessment of requirements that are used to determine detailed application design.

2. The following table identifies the responsibilities associated with these services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Act as the primary point of contact with the business to define, gather, refine, and prioritize business requirements.	X	X
2	Develop and document business requirements	X	
3	Approve business requirements documents		X

#	Key Responsibilities	MSP	GeM
4	Conduct interviews, group workshops and surveys to determine functional and end-user requirements	X	
5	Develop technical requirements to support business and functional requirements	X	
6	Develop functional requirements documents and conceptual data model	X	
7	Develop logical data model	X	
8	Develop physical data model	X	
9	Develop and maintain the traceability matrix for business to functional requirements	X	
10	Maintain the traceability matrix for functional to technical requirements	X	
11	Conduct value assessments of functional requirements and generate an impact analysis, including affected systems, alternative design scenarios, etc.	X	
12	Approve all functional requirements		X
13	Identify the need for software upgrade conversion requirements for Commercial-Off-The-Shelf (COTS) packages and associated hardware	X	X
14	Approve software upgrade conversion requirements for COTS hardware and software		X
15	Recommend and document acceptance test criteria for GeM approval	X	
16	Approve test criteria		X
17	Maintain document repository with all master documents pertaining to all modules and sub-modules stored in a structured manner with proper version control	X	

Table 2: Application req. specifications & business analysis resp. matrix

3.1.2.6   Application Solution Design

1. MSP will perform Application Design Specification Services to produce design specifications, the technical design, formal estimates of the scope and work (effort, duration, cost, and schedule) for application build, and the production of documentation required for phase completion and approval that meet GeM's technical architectural standards and identify and describe the most cost-effective solution to the implementation option under consideration. MSP shall:

a. Incorporate GeM's architectural guidelines into the design, including application extensibility, maintainability, scalability, robustness, reliability, and reusability.

b. Obtain GeM oversight and approval through coordination with the appropriate GeM architectural or technical oversight authority.

2. The following table identifies the responsibilities associated with the high-level application solution design services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Define design standards and documentation	X	
2	Create the detailed design document with support from GeM from the business and functional and non-functional requirements and high-level design	X	
3	Create a design to contain security features in compliance with GeM security policies	X	
4	Provide planned technology design that specifies all components, program modules, data stores, interfaces, interface components and associated operations procedures for the application	X	
5	Document and present implementation options evaluated as required by the requirements document to support the GeM Custom Code process	X	
6	Review and approve detailed design documentation		X
7	Document the logical data model	X	
8	Document technical requirements and physical data model	X	
9	Review and approve technical requirements and physical data models for consistency with documented requirements		X
10	Develop and implement rigorous automated Unit Testing cases, with the goal of their reuse in subsequent Regression Testing	X	
11	Define implementation and deployment policies and staffing requirements to meet deployment and delivery requirements	X	
12	Provide schedule estimates	X	
13	Maintain document repository with all relevant documents stored in a structured manner with proper version control	X	

Table 3: Application solution design responsibility matrix

3.1.2.7 Application Build and Configuration Services

1. Programming and/or Development Services are the activities associated with constructing custom software applications, setup and configuration of software packages, and development of all necessary system-to-system integration components. Application build includes building, execution, unit testing, formal estimates of scope and work (effort, duration, cost, schedule) for the QA Services following the build, and production of documentation for phase completion and approval.

2. The following table identifies the responsibilities associated with these services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Review GeM's existing technical standards	X	
2	Recommend development and technical documentation policies, procedures, and standards in conformance to GeM requirements where applicable	X	
3	Review and establish programming, development, and technical documentation policies, procedures, and standards	X	
4	Perform all necessary technical design, programming, development, automated unit testing, scripting, configuring, or customizing of application modules as required to develop and implement the design plans and specifications	X	
5	Run automated testing such as unit testing, functional testing, security testing, integration testing, etc. periodically as part of the build process, to get fast feedback on the quality of the code	X	
6	Perform application database administration functions	X	
7	Recommend modifications and performance-enhancement adjustments to system software and utilities based on GeM performance standards	X	
8	Manage all programming and development efforts using industry-standard project management tools and methodologies	X	
9	Conduct predetermined development status reviews and provide written reports on results to GeM	X	
1	Deliver all applicable documentation such as High Level	X	

0	Architecture, High Level Design, Low Level Design, System Requirement Specification, test scripts, code, and all other artefacts as mutually agreed with GeM		
1 1	Regularly inform GeM about the build progress and demo the artefacts which will be delivered at the end of the build phase (show & tell sessions)	X	
1 2	Create concept paper for code security mentioning traceability and code ownership sanctity mechanism	X	
1 3	Implementation of code security standards	X	
1 4	Maintain document repository with all relevant documents stored in a structured manner with proper version control	X	

Table 4: Application build and configuration services responsibility matrix

Other related requirements are mentioned below:

1. The identified personnel need to be based at the GeM's office / other designated locations during the entire project duration as mentioned in Volume 1 Section 3.3 of this RFP.

2. While developing the application and carrying out ongoing maintenance, the MSP is required to comply with the processes per CMMi Level 5 and Agile/ Iterative Methodology.

3. The application software developed by the MSP must be based on responsive web design principles and user friendly so that users can access it without having extensive training.

4. The lifecycle for each phase should be independent, i.e., different teams should work in parallel to complete the track activities per the given timelines.

5. Go-Live: The GeM system will be considered as "Live" based on the criteria defined in Volume 1 Section 3.1.2.9.

6. The MSP will be responsible for supplying all the required licenses (including development, test, and production licenses) of the application and related software products as well as subsequent installation to meet system requirements. All such licenses shall be in the name of GeM, or MSP if directed by GeM. All licenses in the name of MSP shall be transferred to GeM before the expiry/ termination of the Agreement or at any other time period as directed by GeM. GeM shall reserve the right to continue or discontinue licenses, including but not limited to licenses pertaining to COTS software, at its discretion post expiry of Agreement.

7. The MSP shall perform periodic audits to measure license compliance against the number of valid End-User software licenses and ensure consistency with the terms and conditions of

license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The MSP shall report any exceptions to license terms and conditions at the right time to the GeM. However, the responsibility of license compliance solely lies with the MSP. Any financial penalty imposed on the GeM during the Agreement period due to license non-compliance shall be borne by the MSP.

8. The MSP shall be following DevOps principles and will be deploying tools and processes required for the same.

9. The MSP shall also supply any other tools & accessories required to complete the integrated solution per requirements. For the integrated solution, the MSP shall supply:

   a. Software & licenses

   b. Tools, accessories, documentation and prepare a list of items supplied. Tools and accessories shall be part of the solution. The Service Provider should provide a technologies matrix.

10. System Documentation: System Documentation both in hard copy and a soft copy will be supplied along with licenses.

11. The indicative sizing considerations for the GeM are given in Volume 1 Section 8.4 of this RFP.

3.1.2.8 Testing/Quality assurance

The MSP shall provide the testing strategy including the traceability matrix and relevant test cases and shall also conduct the testing of various components of the software developed/customized along with the solution as a whole. The testing should be comprehensive and should be carried out at each stage of development as well as implementation.

The MSP shall demonstrate the testing criteria outlined in the table below before Go-Live as well as during the project operations phase. In case required, parameters might be revised by GeM in mutual agreement with the MSP and the revised parameters shall be considered as the Acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

The section below depicts the details for the various kinds of testing activities required for each phase of the project:

The Services described in this Section shall be referred to as the "QA Services." MSP shall provide the QA Services for all solution components. QA Services are a systematic, planned set of actions necessary to provide confidence that the software development and maintenance processes of the ADM Services conform to established functional and technical requirements as well as with the managerial requirements of keeping the schedule and resources within budgetary confines.

MSP shall perform the QA Services throughout the entire SDLC. QA Services include the following:

1. A quality management approach

2. Effective software engineering technology (methods and tools)

3. Formal technical reviews applied throughout the SDLC process

4. Multi-tiered application integration and testing strategy, and implementation

5. Control of software documentation and the changes made to it

6. A procedure to measure compliance with software development standards

7. Measurement and reporting mechanisms

The following table identifies the responsibilities associated with these Services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Provide appropriate visibility into the QA Services processes that MSP uses, and visibility of the results as related to the Application being worked upon	X	
2	Setup a system with capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.	X	
3	Validate that all the activities necessary to design, develop and implement any Changes are not only effective and efficient for quality assurance and control but geared toward continuous quality improvement	X	
4	Support and suggest improvements for all Acceptance Testing Services conducted by GeM	X	
5	Provide and maintain tooling (incl. licenses) related to the QA Services	X	

Table 5: Testing/Quality assurance responsibility matrix

3.1.2.8.1 Build Verification Services (Application Integration and Testing)

The Build Verification step is considered part of the Build phase and thus part of the sprint. Build Verification includes verifying the code quality, the refinement of test cases, the execution of test cases, the provision of supporting tools, equipment and environment and the production of documentation for phase completion and approval.

The purpose of this phase is to demonstrate that the software developed satisfies all the software requirements in the requirements document. This phase shall include testing for system-level functionality, security, performance, external interfaces, usability, and integration of the different modules. All the different types of testing should be automated to the extent possible.

MSP will involve the GeM Technology owners, Functional owners and Application Owners early in the process, to allow a fast feedback loop in the validation of the quality of the delivered work of the sprint. It is up to MSP to set up and manage this close collaboration. Detecting issues early in the process will result in fewer cycles and is beneficial for either party.

The following table identifies the responsibilities associated with these Services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Execute automated static code analysis and verify no blocking or major issues are detected	X	
2	Manual code review, to verify the code quality and to verify if code is compliant with agreed conventions, standards, and best practices	X	
3	Possibility to participate in the code review		X
4	Develop an overall test plan that documents the test strategy, test coverage, test scenarios, test bed, test data, test methods, test schedule and responsibilities to accomplish quality assurance of the affected system	X	
5	Provide and manage a test environment with either scrambled real-time production data or relevant generated test data. This test environment should allow the execution of all test categories defined in this section.	X	
6	Mask the test data for sensitive information	X	
7	Create test cases and suitably use the existing data to generate new test data to perform all appropriate testing, including Assembly Testing, End-to-end Testing, Stress Testing, Regression Testing, Cross-browser/platform testing	X	
8	Conduct technical smoke tests	X	
9	Conduct functional smoke tests, e.g., story testing	X	
10	Support functional smoke tests		X
11	Conduct Regression Testing per test plan requirements	X	
12	Conduct system testing per test plan requirements	X	

13	Conduct cross-browser / cross-platform testing if appropriate	X	
14	Automate test scenarios as much as possible, to a certain extent	X	
15	Provide shared access to the mutually agreed defect tracking system for purposes of allowing GeM to initiate, track, and the report found defects (e.g., user acceptance testing)	X	
16	Correct defects found as a result of testing efforts	X	
17	Develop, document, and maintain in the Policies and Procedures Manual integration and testing procedures that meet GeM requirements and adhere to policies defined by GeM	X	
18	Maintain software release matrices across development, quality assurance, and production environments and networks	X	
19	Provide and support in-scope application associated middleware required to integrate software and hardware	X	
20	Perform configuration management and Change management activities related to integration and testing	X	
21	Continuously improve the testing services, for example by introducing new automated test approaches or any other improvements	X	
22	Maintain document repository with all relevant documents stored in a structured manner with proper version control	X	

Table 6: Build verification services responsibility matrix

3.1.2.8.2   Handover from Build Verification to Acceptance testing

Before delivering to GeM any Deliverable, MSP shall (a) complete appropriate testing to ensure that the Deliverable meets the applicable quality acceptance criteria and (b) submit the results of such testing to GeM for preliminary review. MSP shall provide GeM with access to proof and all results of such required deliverables, documentation, code review, testing, test data and testing tools so that GeM may ascertain that the applicable quality acceptance criteria have been met during GeM's review of the Deliverable in accordance with the agreed standards. GeM shall also have the right during such period, at its sole discretion, to replicate the testing conducted by the MSP, or to conduct additional testing, or to request additional quality services, to determine whether the Deliverable conforms to the applicable quality acceptance criteria.

3.1.2.8.3   Application Acceptance Testing

The following Services shall be in scope for the application Acceptance testing phase:

1. Prepare GeM QA environment, including relevant data and configuration

2. Migrate code approved by GeM to GeM source code control; move code approved by GeM to QA

3. Support GeM User Acceptance Testing (UAT) team(s), if applicable.

4. Conduct Performance and Load testing

5. Conduct Security Testing

6. Provide Reports which prove conformance with the non-functional requirements

All the different types of testing should be automated to the extent possible.

The following table identifies the responsibilities associated with these services. An "X" is placed in the column under the Party that will be responsible for performing the task. MSP responsibilities are indicated in the column labelled "MSP."

#	Key Responsibilities	MSP	GeM
1	Confirm testing environment appropriately matches GeM's production environment including DB schemas and DB list of users. Ensure complete segregation via air gap between testing and production environment. Apply project code from GeM source code repository	X	
2	Provision and maintain the Acceptance Test environment	X	
3	Release and deploy signed-off code to GeM's Acceptance Test environment. Support compilation and configuration, as appropriate	X	
4	Manage the relationship with all interfaced systems necessary to conduct the test, perform troubleshooting, simulate interfaces or work with integrated systems to conduct Acceptance Testing, support batch processing, exercise functionality, and report results.	X	
5	Verify and approve the Acceptance Test environment		X
6	Work jointly to formulate an Acceptance Test Plan and process.	X	X
7	Define and prepare sufficient qualitative test cases for the Functional Acceptance Testing for each of these types: story testing, core functional testing, end-2-end integration testing, end-2-end regression testing, end-2-end functional testing	X	

#	Key Responsibilities	MSP	GeM
8	Define and prepare sufficient qualitative test cases for the User Acceptance Testing for each of these types: usability and user experience testing, story testing, end-2-end functional testing	X	
9	Provide a test data repository with relevant data for the new or updated functionalities	X	
10	Provide assets and devices for cross-platform or cross-browser testing if relevant	X	
11	Provide correct access for GeM personnel to execute Functional Acceptance Testing and User Acceptance Testing	X	
12	Execute Functional Acceptance testing	X	X
13	Execute User Acceptance testing	X	X
14	Support GeM execution of Acceptance Testing including issue investigation and resolution	X	
15	Conduct Performance and Load Testing	X	
16	Conduct Security Testing	X	
17	Provide Reports which prove conformance with the non-functional requirements (responsiveness, transaction times, scalability, security, maintainability…)	X	
18	Perform defect management: 1. Resolve all applications or database problems that require database, application code and/or operational modifications as a result of error correction 2. Identify application, performance and/or database problems 3. Notify vendor of such problems 4. Arrange for the corrections to be made. If it is MSP software, MSP shall make the corrections 5. Coordinate the corrections according to the agreed severity prioritization criteria and correction process 6. Test the corrections 7. Schedule the installation of the corrections into the product test environment per the change control procedures 8. Submit the change to the product test environment in accordance with the change control procedures	X	
19	Support and respond to change requests	X	

#	Key Responsibilities	MSP	GeM
20	Prepare deployment plan, including release management process	X	
21	Participate in Acceptance Test approval process	X	
22	Complete updated support documentation (e.g., user manuals, training material, FAQ, new features, etc.) and train GeM support staff	X	
23	Manage UAT process with internal business users		X
24	Receive and review updated documentation		X
25	Provide a neutral point of contact to obtain the test preparation and to monitor the test progress of the Acceptance Testing phases. This SPOC will provide GeM with real-time test progress reports	X	
26	Continuously improve MSP's activities, processes and tooling linked to the Acceptance Testing phases.	X	
27	Propose improvements to GeM's activities, processes and tooling related to the Acceptance Testing phases.	X	
28	Maintain document repository with all relevant documents stored in a structured manner with proper version control.	X	

Table 7: Application acceptance testing responsibility matrix

Note:

1. The MSP needs to provide the details of the testing strategy and approach including details of the intended tools/environment to be used by the MSP for testing in its technical proposal.

2. The MSP must ensure the deployment of necessary resources and tools during the testing phases. The MSP shall perform the testing of the solution based on the approved test plan, document the results, and shall fix the bugs found during the testing. It is the responsibility of the MSP to ensure that the end product delivered by the MSP meets all the requirements specified in this RFP. The MSP shall take remedial action based on the outcome of the tests.

3. The MSP must ensure that developers or development team should not have the access to Acceptance testing environment as frequent changes impact the testing quality.

4. GeM reserves the right to appoint third-party agencies/ auditors for the purpose of User Acceptance Testing. All the Third-Party Auditors (TPA) will be appointed and paid by GeM directly. All tools/environments required for testing shall be provided by the MSP. The MSP needs to prepare and provide all requisite information/documents to a third-party auditor and ensure that there is no delay in the overall schedule.

5. Post-Go-Live, the Production environment should not be used for testing and training purposes. If any Production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirements should be provided by the MSP in its technical proposal. The process will be finalized with the MSP and GeM.

6. The cost of rectification of non-compliance shall be borne by the MSP.

3.1.2.9 Go-Live preparedness and Go-Live

1. The MSP shall prepare and agree with GeM on the detailed plan for Go-Live and ensure that it is aligned with the implementation schedule as defined in Volume 1 Section 5 of this RFP. The plan must include the completion of the Testing activities as mentioned in Section 3.1.2.8.

2. The MSP shall ensure that all the data migration is done from the existing GeM System in alignment with GeM and the system is released for the operations.

3. MSP shall submit a signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

4. Set up and deployment of Production Infrastructure, network and security components should be completed and approved by GeM.

5. The application should be deployed successfully in the production environment.

6. Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

7. There will be a post Go-live monitoring phase for every feature which will be a minimum of 7 days where it will be monitored that the feature is functioning seamlessly, integrations are properly in place and performance is being maintained at requisite levels. During this period, daily reports on the feature performance will need to be supported by MSP

8. The Go-Live plan to be prepared and submitted by the MSP should include a detailed Go-Live Criteria. The completion of Go-Live stage shall be subjected to MSP completing all the requirements listed in the Go-Live criteria and GeM reviewing and approving the same. The Go-Live criteria should, at a minimum, include the following:

    a. Design, development, testing and deployment of the following in the production environment:

        i. New GeM web platform and Mobile Webapp (including all modules mentioned in Volume 1 Section 8.1 of this RFP)

        ii. GeM mobile app with real-time reporting, alerts / notification and user

authentication features

    iii.   Data analytics and BI tool with advanced analytics/ AI/ML use cases, dashboards and reports aligned with GeM during design phase

    iv.   All external integrations currently live on GeM (e.g., UIDAI, GSTN, Income Tax Department, MCA-21, PFMS, IFMS, etc.) as mentioned in Volume 1 Section 8.1.18 of this RFP

    v.   CRM solution as described in Volume 1 Section 3.1.7.1 and 3.1.7.10 of this RFP

    vi.   SLA and Payment Management tool in Volume 1 Section 6.2 and Section 8.6.3 of this RFP

    vii.   Change management tool as described in Volume 1 Section 8.7.3 of this RFP

b.   Completion of data migration from existing to new GeM platform

c.   Onboarding, deployment and training completion of all named resources as mentioned in Manpower requirements section, Volume 1 Section 8.5.1 of this RFP *(including trainers, business facilitators, marketing executives, contact centre executives)*

d.   Operationalization of contact centres, including facilities, deployment of trained resources, infrastructure, and CRM solution, as mentioned in Volume 1 Section 3.1.7 of this RFP

e.   Submission and approval from GeM on all documentation (e.g., BRD, FRS, SRS, HLD, LLD, etc.), as aligned with GeM, and storage of documentation in a digital repository with proper version control

3.1.2.10   Data Migration

MSP shall be responsible to migrate the data from existing GeM platform to new GeM platform seamlessly, and must perform the activities including, but not limited to, data profiling, cleansing and migration as detailed below. Additionally, MSP shall submit a detailed Data Migration Plan as mentioned in Volume 1 Section 5 of the RFP which shall be reviewed and approved by GeM.

3.1.2.10.1   Data Profiling

1.   MSP shall conduct a data audit against all identified data sources identifying the data that needs to be corrected

2. MSP shall provide a data analysis report from the data audit (e.g. description of problem, data source, number of occurrences, missing data, impact on production data)

3. MSP shall identify who will be responsible for correcting the data elements that are in error, along with an explanation as to how they came to this conclusion

4. MSP shall ensure the data rules are in compliance with the GeM rules, policies and statutes

5. MSP shall identify problems including, but not limited to:

a. duplicates;

b. missing primary-foreign key relationships;

c. redundant data;

d. soundex matches for the same data;

e. incorrect formatting;

f. incorrect data based on a numeric range;

g. incorrect data based on relationship rules;

h. non-unique keys;

i. missing data;

j. incomplete data elements based on GeM business rules, policies and statutes;

k. referential integrity;

l. orphaned records (records that should be associated to others but are not);

m. childless parents (records that should have related records but do not) based on GeM business rules, policies and statutes;

n. data value commonality (same code used multiple places with varying values);

o. invalid date ranges (when the dates do not conform to business or logical standards);

p. invalid/incomplete dates;

q. invalid code values;

r. code value outliers outside of expected values;

s. code value anomalies based on GeM business rules, policies and statutes;

6. MSP shall provide the criteria for the data sampling for the data audit (e.g. class, group, status, age).

7. Document and meta data compatibility to be assessed and ensured

3.1.2.10.2   Data Cleansing

1. MSP shall provide a method of correction for elements identified as a result of Data Profiling.

2. MSP shall ensure the data is cleansed according to administrative rules, statutes, policies and agency business rules.

3. MSP shall conduct ongoing data audits against all identified data sources during the cleansing process.

4. MSP shall provide a data analysis report from the data audit (e.g. description of problem, data source, number of occurrences, impact on production data, type of fix that was applied, number of records fixed, and number of records unable to be fixed).

5. MSP shall provide a prioritized list of data elements to be cleansed.

6. MSP shall provide an on-going data cleansing maintenance plan.

7. MSP shall provide a Quality Assurance/Audit plan to ensure counts, dollars, etc.

8. MSP shall retain history (audit trail) of all data elements that are changed through cleansing (before and after).

9. MSP shall provide reconciliation reports between Core system and the Staging Database.

10. MSP shall develop scripts needed to populate the staging database.

11. MSP shall produce a data mapping schema for all the data sources being used to load the staging database.

12. MSP shall produce a data dictionary for the staging data database.

13. MSP shall produce a data model of the staging database.

3.1.2.10.3   Data Migration

1. MSP shall produce a data mapping schema for the staging database and all the data elements being used to load the new GeM database.

2. MSP shall produce a data mapping schema for the Cleansing Exception database and all the data elements that were not able to migrate to the new GeM database.

3. MSP shall conduct a data audit against all identified data sources during the migration process from the staging database to the new GeM database.

4. MSP shall provide a data analysis report from the migration data audit (e.g. description of problem, data source, number of occurrences, impact on production data).

5. MSP shall provide the testing process, including the test plan, test cases, test scenarios and expected results for the migration from the staging database to the new GeM database.

6. MSP shall perform data mock conversions as part of its testing.

7. MSP shall develop of scripts needed to populate the cleansing exception database.

8. MSP shall retain history (audit trail) of all data elements that are changed through migration.

9. MSP shall continue to perform data cleansing for those records that were identified as being incorrect during the migration and testing process.

10. MSP shall provide GeM with a quality assurance/audit process and reconciliation report that validates migrated data from the Staging database to the new GeM database and the Cleansing Exception database (contains the records that cannot be cleansed).

3.1.3 External integration

Integration with 3rd party – outbound

1. In order to integrate the platform with 3rd party systems like PAN, Aadhar, payments and other system – MSP should develop plugin framework with well-defined data interchange standards, and well-defined request signatures that others can use to integrate with the GeM platform

2. Integration to 3rd party services should be allowed through a defined contract's (channel adaptor) implementation

3. The target platform should employ proxy pattern to integrate with 3rd party system by defining a proper contract layer. The implementation of these proxy should be separated from the domain service ensuring loose coupling between invocation from domain service to 3rd party system and its implementation

4. In order to integrate with 3rd party systems, the GeM platform should standardize the request and response structure in order to keep the backend design stable without adoption to multiple 3rd party systems.

5. The implementation for the adaptor should be such as not to disrupt the changes to domain

services.

6. An integration with PAN or GST number should be modeled as a generic "tax identifier" integration. Appropriate plugins/ adaptors should be created to then do the actual integration.

7. MSP shall ensure that all integrations must comply with all relevant GoI/ ministry/ department guidelines such as RBI security guidelines

Integration with 3rd party – inbound

1. Platform should support an interoperability framework with:

   a. Well defined data interchange standards

   b. Well defined Master Data Codes, and

   c. Well-defined request signatures that others can use to integrate with the GeM platform.

2. Target platform should agree on defining standard interfaces, data-formats and protocols.

3. Exposing data and services as web-services which should allow users to access and integrate with the services.

4. Any 3rd party integration should happen only via such interoperability standards, and through the common API gateway.

5. MSP shall ensure that all integrations must comply with all relevant GoI/ ministry/ department guidelines such as RBI security guidelines.

3.1.4   Cloud Provisioning & Commissioning

The MSP shall be responsible for deploying the entire GeM solution on a Cloud, either through in-house capabilities or a Cloud Service Provider (CSP) meeting the eligibility requirements as specified in Volume 2 Section 2.2 of this RFP.

Detailed scope for cloud services has been laid out in Volume 1 Section 8.3 of this RFP. All the requirements/scope of work mentioned in this section shall be the responsibility of the MSP. In case of a consortium bid, the Lead bidder shall ensure fulfilment of responsibilities laid out in Volume 3 Section 24 of this RFP including that the CSP provides the following features in the cloud and also performs the scope of work that is directly attributable to CSP.

3.1.5 Establishment of Network Connectivity

1. The MSP shall provide Internet and MPLS bandwidth (over VPN) at GeM Offices, Contact Centre & Technical Helpdesk sites, CSP DC & DR sites, and for integrations with external parties such as NIC (as applicable).

2. The MSP shall provide the network connectivity (with Internet) at all aforementioned locations from two different network Service Providers for redundancy via a tripartite agreement between GeM, MSP and network service provider.

3. The MSP needs to size and provide appropriate bandwidth along basic customer-end equipment at the aforementioned locations required for terminating the network connectivity at these locations.

4. Any connectivity provided should be over P2P (Private links) including VPN over private links. Public network link must be avoided.

5. Bandwidth estimation is to be completed by the MSP based on the data replication requirements, user projections for the entire Agreement duration and compliance with the service levels. The MSP needs to provide details of bandwidth sizing at each location in the technical proposal. The MSP needs to meet the service levels as mentioned in Volume 1 section 8.6 of this RFP.

6. The MSP shall provide the detailed Bandwidth calculation, monitor all network links for this project, and ensure that bandwidth utilization does not cross 70% at any point of time.

7. The MSP, through EMS, should also provide network related reports including following:

   a. Link up/down (real-time as well as periodic).

   b. Link utilization in % (real-time as well as periodic) (Link utilization should not be more than 70% in each case, barring acceptable occasional surges).

   c. Router up/down (real-time as well as periodic).

   d. Top and Bottom N graphs showing the best and worst links in terms of availability (periodic).

   e. Reports on threshold violations- Functionalities for setting thresholds and getting alerts on threshold violations should be embedded in the system. (real-time as well as periodic)

   f. Bandwidth utilization report for each link along with utilization trends. The report should have capabilities for displaying the minimum, maximum and average for each link (real- time as well as periodic).

g. The monitoring solution provides for application/port level traffic analysis with source and destination identifications.

h. Report on jitters and latency due to network parameters, closely linked to reachability shall be available (real-time as well as periodic).

i. Router Statistics: CPU utilization and free memory reports of all the routers in the network should be available. Memory and CPU utilization reports will show maximum and minimum against a predefined threshold.

3.1.6 Application Training and Capacity Building

The MSP will prepare a training portal as part of the GeM Solution to provide training to the Portal users.

1. Finalization of Training plan and strategy

2. Provisioning of multi-lingual Learning Management System (LMS) in the following languages: English, Hindi, Assamese, Bengali, Garo, Gujarati, Kannada, Khasi, Konkani, Malayalam, Manipuri, Marathi, Nepali, Oriya, Punjabi, Tamil, Telugu and Urdu

3. Preparation of a repository of training material including Computer Based Trainings (CBTs) – audio/video, presentations, Functional flow documents, FAQs, etc. and periodic updates to these artefacts, with proper version control, for following stakeholders, at minimum –

    a. GeM- officials

    b. GeM- internal users

    c. GeM- system administrators

    d. Third-party agencies

    e. Current and potential Sellers/ Service Providers

    f. Current and potential Buyers

3. As and when required Classroom training for the following stakeholders -

    a. GeM- officials

    b. GeM- internal users

    c. GeM- system administrators

4. MSP should nominate personnel who have the right mix of technical and domain experience to impart the training.

5. The MSP shall be required to provide training to departmental users notified by GeM on a time-to-time basis, with a batch size decided by GeM.

6. These trainings can be arranged any time after UAT till completion of duration of the Agreement.

7. The Scope of Work that needs to be undertaken by the MSP for imparting training is given below. The proposed training module is expected to help the Course takers and other stakeholders, including GeM officials, to undertake their revised roles and responsibilities with ease and without any apprehensions.

8. The MSP must assume the following responsibilities:

   a. The MSP shall provide training to all the stakeholders. The training days can be revised by GeM based on the requirement.

   b. The MSP needs to conduct a 'Training Needs Analysis" (TNA) and impart Training to the Users as per the Groups defined above, according to their individual needs and requirements.

   c. The schedule/training calendar shall be provided to the MSP by GeM and the training material for imparting the trainings shall be developed by the MSP in consultation with GeM. The MSP shall submit a softcopy and hardcopy of the training material to the GeM Team before every training session.

   d. In case of need for modifications in the Training Plans or substitutions of the regular trainers, proper correspondence with the GeM Team shall be made.

   e. The training program shall be continuously monitored by GeM so as to ensure quality standards of the Training. It is the responsibility of the MSP to prepare a feedback mechanism (i.e., printed feedback forms, online feedback mechanism) and get it filled by the participating batch and submit the same on a regular basis to GeM Team, along with an assessment of the trainers themselves.

   f. A detailed training schedule/ calendar, including the dates, participants, areas to be covered, time, mode of training, language, location, etc. shall be provided to the MSP by GeM, the training literature shall be supplied by MSP at various stages of the project cycle, and feedback for effectiveness will be agreed to by all parties during the performance evaluation of the MSP as per the Agreement.

   g. Trainings shall be provided as per the training schedule provided by GeM.

h. It is the responsibility of the MSP to prepare documents including User manuals, technical manuals, and administration manuals, and provide the same to the GeM Management team. The team will provide the necessary inputs for preparing the training material.

i. Audio Visual Training system - The MSP is also required to provide multi-lingual Audio-Visual Trainings to the users for assistance in operating/navigating through the Portal. The module/ sub-module/ section-wise training material, especially in form of Audio-Visual content or animation, apart from the PDF version, have to be uploaded in each module/ sub-module/ section of the Portal which can be played at any given point of time through the browser. The users should find it easy to understand the process and functionality better by seeing the audio-visual training content for that specific module/ sub-module/ section and work accordingly as required. MSP shall also maintain a module/ sub-module/ section-wise training material repository with proper version control. The master documents/ audio-visual files shall be updated periodically to ensure latest changes are accurately reflected in the training materials.

j. These Audio-Visual clips will have the functionality to start, stop, pause, rewind, forward, and playback speed adjustment options, so that the user can play the training content as per his own free will and requirement. All these specific module/sub-module/section-wise audio-visual training content should be integrated to form a complete training of the Portal and uploaded on the portal for free access, download and ready reference.

k. Online Help/Reference with Search option - It is also proposed that the training contents and user manuals will be made available to users in downloadable (PDF) format so that the users may refer/ download it for their own personal reference as and when needed. It is required that the downloadable training content should have proper indexing and internal references, mapped to keywords in order to allow any user to search and reach the desired content with the help of those keywords. It is envisaged that any user will be able to search and read the directions/ information for only the part required by him/ her rather than looking through the entire PDF document and manually searching for the right content.

l. On entering the keywords for search criteria, the system should pull out and display the links to the content as mapped. This feature should be dynamic with real-time search availability, i.e., as soon as the keywords are changed; a new set of content links with page/ chapter references within the document should appear for selection. Once the selection is made by the user, the system should display the PDF content.

m. All the training material, including but not limited to, user manuals, technical manuals, and administration manuals, and audio/ video content shall be translated

and provisioned by MSP across multiple languages used across states in India for Buyer and Seller/ Service Provider convenience. Languages to be included are as follows: English, Hindi, Assamese, Bengali, Garo, Gujarati, Kannada, Khasi, Konkani, Malayalam, Manipuri, Marathi, Nepali, Oriya, Punjabi, Tamil, Telugu and Urdu.

9. Design suitable paper-based/ online or practical tests for assessment of the trained participants especially on the use of Applications, IT infrastructure, basic troubleshooting etc. The vendor will have to get the same approved from the Government entity/ department.

10. Use various predefined Forms for gathering feedback regarding the satisfaction of trained participants. The feedback should focus on the relevance of course content/coverage, quality of presentation, quality of training material provided, relevant examples/practice sessions, quality of faculty, administrative arrangements done for the training, etc.

3.1.7 GeM Contact Centre & Technical Helpdesk Operations

The GeM system will also require an inbound/ outbound Contact Centre. The MSP shall set up and run the GeM Contact Centre for GeM (onboarding kick-off to be done by 6 months prior to the date of expiry of outgoing MSP's contract as mentioned in Volume 1 Section 5 of the RFP with select resources and systems; Ramp up & transition to be done in a phased manner between 6 months prior to the date of expiry of outgoing MSP's contract and date of complete take over of maintenance and operations of existing GeM platform by incoming MSP as defined in Volume 1 Section 5 of the RFP) till the end of Agreement duration as defined in this RFP.

1. To ensure business continuity, minimum 2 contact centre facilities shall be set up. These facilities can be set up in different cities, with at least one contact centre facility in Delhi NCR region (minimum 60% resource capacity in this facility) to ensure efficient collaboration between GeM and the contact centre team.

2. The MSP shall setup all required infrastructure for the operations of the contact centre.

3. The MSP shall provision a contact centre for both internal and external users.

4. The MSP shall provision a chatbot on the portal with functionality and enough literature to address and resolve basic queries at source and redirect to call centre agents in case of non-resolutions.

5. The Contact Centre and chatbot shall support languages as specified in the next section.

6. The MSP is required to meet the SLAs of Contact Centre as listed in Volume 1 Section 8.6 of this RFP.

7. Contact centre shall service GeM stakeholders in different geographical regions in India.

8. Every call received/ done from the call centre would be recorded in the call centre application against the respective ID.

9. Each call would have a unique identifier and in case there is any query/grievance/any other request, stakeholder shall be intimated about the Ticket ID for future tracking purpose.

10. To ensure Customer Service Quality, GeM shall conduct regular audits, random audits, and call barging.

11. The Contact Centre will majorly receive requests or queries in the areas including, but not limited to, the following:

    a. Buyer registration

    b. Seller/ Service Provider registration

    c. Inspection related queries

    d. Procurement process related queries: L1 purchase, Bids, Reverse Auction, BoQ, etc.

    e. Payment status or queries

    f. IT-related issues

    g. Grievance Redressal (Sellers, Service Providers, Buyers, etc.), etc.

    h. Third party integrations

12. The MSP shall deploy a CRM Solution for Contact Centre Operations as specified below.

13. In case of sub-contracting of contact centre, the sub-contractor must be a company, preferably a public limited company, with at least 5 years of legal existence.

3.1.7.1.   Deployment of CRM Solution for Contact Centre Operations

1. The MSP shall design, supply, customize, commission, and deploy a CRM system based on GeM's requirements, for Contact Centre Operations.

2. The CRM solution is expected to be a single-window grievance redressal mechanism for the GeM system. The scope shall include any customizations of the CRM solution as per GeM's requirements and associated Software Lifecycle Services.

3. MSP shall be responsible for operations, maintenance and support of CRM solution and its associated updates and upgrades. The warranty and AMC proposed should cover the duration

of the Agreement.

4. The MSP shall be responsible for integrating the CRM with the entire GeM Solution and ensure the health of the integration. MSP shall also provide and manage access to CRM to appropriate users in alignment with GeM.

5. MSP shall analyze the requirements of IT infrastructure for hosting of the CRM software to meet the availability, performance and response times required for industry-standard CRM solutions.

6. MSP shall provide CRM Reports on a daily, weekly, monthly, quarterly, and yearly basis, detailing, but not limited to, outstanding issues, grievances, and application status of residents.

3.1.7.2 Key features of the proposed Contact Centre

The key features of the proposed Contact Centre are enlisted in the table below:

No. of Seats	**6 months prior to date of outgoing MSP's contract expiry:** Starting with 70 seats for inbound and 20 seats for outbound **Date of complete take over of maintenance and operations of existing GeM platform by incoming MSP:** Min. 200 seats for inbound and 30 seats for outbound **Beyond date of complete take over of maintenance and operations of existing GeM platform by incoming MSP:** Actual number as per capacity planning for all channels in agreement with GeM Number of seats per language and per desk (L0, KNE – contact center escalations and GeM official escalations, L1, L2) to be finalized in mutual alignment with GeM before Go-live. Capacity plan shall be shared by MSP for all types of resources (L0, KNE, L1, L2, team leaders, language wise resources, inbound & outbound resources, etc.) 60 days prior to the start of the month, for every month.
Languages supported	English, Hindi, Assamese, Bengali, Gujarati, Marathi, Kannada, Malayalam, Telugu, Odia, Punjabi, and Tamil.
Operations	6 days a week (Monday – Saturday) 9:00 AM to 10:00 PM The timings and working days of the contact center may be revised by GeM as per business requirements in the future.

Accessibility	Accessible through a Toll-Free Number, IVR Solution, webchat, GeM portal, e-mail, Walk-in desk, WhatsApp *(implementation ongoing)*, etc.
Review	Weekly/ Monthly/ Quarterly business review of call volumes, number of seats required to provide services, business initiatives and value adds
Certification	Contact Centre should be ISO Certified prior to start of operations in this project
Offsite/Onsite	Offsite (process will be operated in an enclosed area within the facility; each facility should have the provision for biometric authentication, video surveillance and seating for at least 2 supervisors from GeM. The surveillance data shall be shared with GeM as requested.)

Table 8: Contact centre features

The Contact centre services would be required for - Inbound & Outbound

1. Inbound

   The inbound calls should include all types of calls received related to technical, business and functional aspects of GeM Solution. The mode of inbound calls should support Voice, Fax, Letters, Web portal, Email, Walk-in desk, etc.

2. Outbound

   The Outbound interactions could be used to respond to queries/grievances of stakeholders not hitherto resolved earlier or for pro-actively obtaining feedback on services delivered.

   a. Calls to ticket requesters

   b. Calls to other stakeholders as specified by GeM

   c. The resolution, status, & updates of complaints, feedback, & IT related calls

   d. Close-looping of tickets: All tickets (non-FCR tickets not resolved real-time by L0, tickets moving to L1/L2, escalations) to be close-looped with customer over call prior to changing the status of the ticket to 'closed'

The contact centre should also support skill-based routing of tickets via formulation of specialized sub-teams to tackle top user issues. The MSP must also provision for a specialized desk in future for large Buyers and Sellers/ Service providers.

The following diagrams represent a simplistic description of the envisaged Contact Centre:
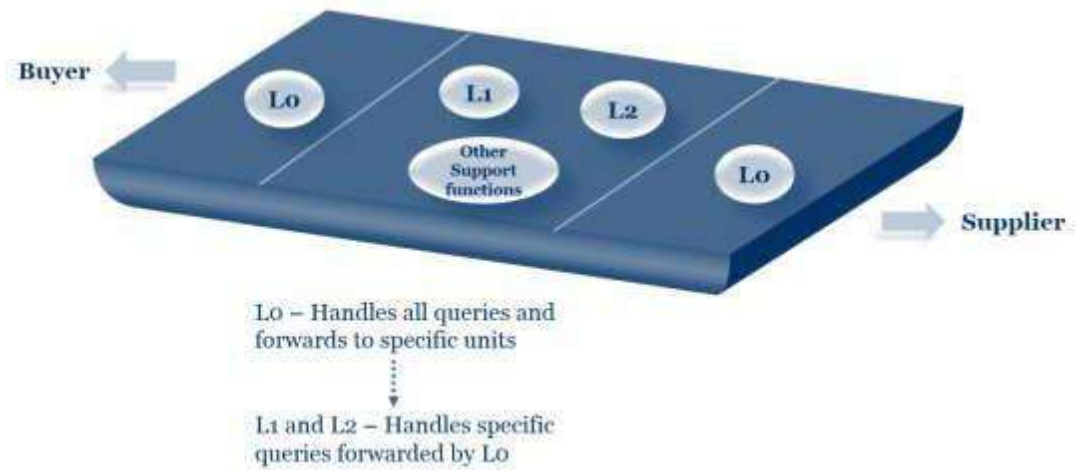
Figure 2: Contact Centre layout
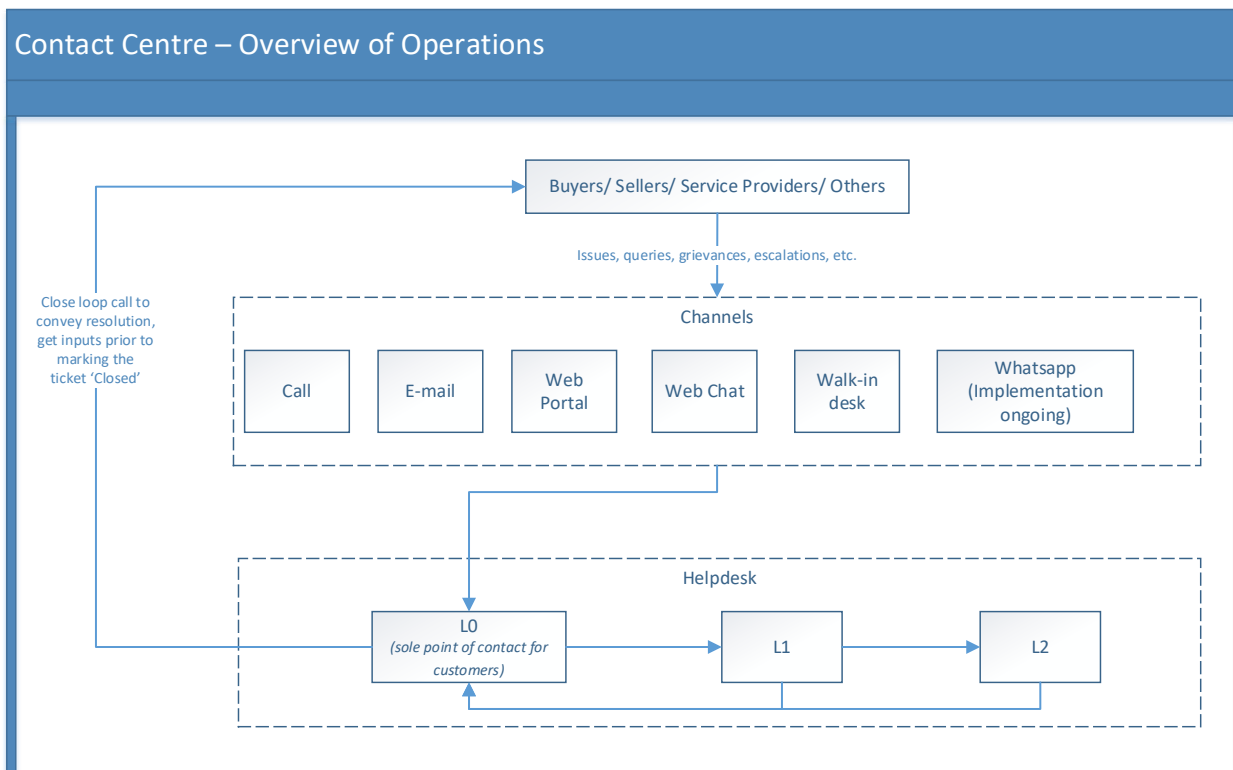
Figure 3: Contact Centre Operations Overview

The Contact Centre will be operated at three different levels as detailed below. All these levels will comprise of MSP/ Sub-contractor's resources.

1. **L0**

   The L0 level will comprise of contact centre agents who will be the first point of contact receiving all queries from the stakeholders as well as supervisory desk agents to manage escalations (KNEs). They will resolve the basic queries there and then and forward the rest to the specific specialized officials at the L1 level.

   Specifically for IT:

   Ability to provide general Product information, hardware and software provisioning, configuration, and technical assistance for installations and upgrades. The focus is on customer issues. L0 Support resolutions are derived primarily from documentation and technical publications. Tier One Support functions include opening trouble reports, collection of relevant technical problem identification information; performing of base problem determination; providing basic support on the standard protocols and features; providing regular problem resolution status reports to the customer and providing the L1 Support provider with problem descriptions which cannot be resolved by L0 Support in accordance with the Performance Measurements identified herein.

2. **L1**

   The L1 level will comprise of agents with in-depth knowledge of technical and non-technical processes/ aspects of GeM and also specialized agents in IT. This level will receive specific queries related to quality, supply, IT, etc. forwarded by the L0 level. L1 resources shall be resources from MSP team and shall be on MSP payroll.

   Specifically for IT :

   The ability to resolve complex customer issues. The focus is also on customer issues. Tier Two Support resolutions require skill to troubleshoot and repair complex hardware and software troubles that can result in partial or complete loss of service. L1 Support functions include correcting the majority of mis-configurations, troubleshooting and simulating complex configuration, hardware, and software problems, supporting problem isolation and determination of documentation errors or Product defects (if possible); defining a problem resolution action plan; doing in-depth analysis of traces and log files, providing support on all protocols and features, diagnosing problems remotely and providing the L2 Support provider with problem descriptions which cannot be resolved by L0 and L1 Support.

3. **L2**

   The L2 level will comprise of high-level agents who oversee the end-to-end process on the portal and also the IT team handling IT related issues/queries. They will address very complex issues that will be forwarded by the L1 agents. Some of the policy-related issues will be required to be forwarded to GeM officials for assistance in resolution, on a need basis. L2

resources shall be resources from MSP team and shall be on MSP payroll. There shall be dedicated team of L2 agents for resolving L2 level issues routed via contact centre channels. These dedicated L2 agents shall not be involved in any other tasks.

Specifically for IT :

Troubleshooting and fixing or generating workarounds for software bugs, where software bugs are described as code or database configuration errors found in the software – limited to code, not including any configuration changes or database changes made by any parties other than Vendor itself. L2 Support is focused on the Product. Tier Three Support will include additional support on all protocols and features supported by the Product, analysis of traces and log files, root cause analysis, installation and configuration support and core dumps for the purpose of fixing software bugs as well as support in troubleshooting issues with respect to any third-party hardware platform on which the Product is running.

The Contact Centre shall provide the following services:

1. **Technical Helpdesk** – For any informational, incidental & operational queries related to IT systems.

2. **Services Helpdesk** – For any informational, incidental & operational queries related to the following but not limited to:

    a. Buyer/Seller/ Service Provider Services (Processes, registration, documentation, etc.)

    b. Inspection Services (Services, charges, process, queries) (only if applicable)

    c. Legal

    d. Grievances

3. **Business operations** – In addition to the helpdesk services mentioned above the Contact centre shall also provide outbound calling services for the scenarios including, but not limited to, the following:

    a. Voice campaigns for spreading awareness about GeM services, promotions, etc. to the registered Buyers and Sellers/ Service Providers & any other list provided by GeM.

    b. Promote inspection through GeM designated Inspection agencies via outbound calling to Buyers once they initiate a transaction (if applicable).

    c. Ensure participation of maximum numbers of bidders through on-call follow-ups with registered bidders.

Technical Helpdesk support: The MSP shall set up a technical helpdesk with qualified personnel to resolve technical queries from Buyers, Sellers, Service Providers, and other stakeholders regarding hardware and software used for implementing processes.

1. Technical queries that will have to be supported by the technical support team will include queries and grievances with regards to PCs, network, and GeM Software.

2. The queries will be answered using a pre-defined script developed in consultation with or provided by respective contractors or GeM/MSP teams.

3. For queries that cannot be answered using a pre-defined script, the query shall be logged in the CRM and tracked to resolution.

4. The MSP shall also be responsible for following up with the entities responsible and updating the resolution status.

5. The CRM solution should support all the requirements of the Technical Support team.

The following are the key activities to be performed by the MSP for Contact Centre Operations:

3.1.7.3 Requirement Analysis and Planning

MSP shall understand the business processes and requirements of GeM Solution and various Services to be provided through the contact centre. This shall include the following activities among others:

1. Preparing a detailed plan for helpdesk set up, with timelines and activities.

2. Preparation of the resource requirement plan for the Services to be provided, including details of experience and skill of the resources required.

3. Identification of the Subject Matter Experts in those technology/process areas.

4. Finalization of Review/ Governance Plan with GeM.

3.1.7.4 Selection and Deployment of Manpower

1. MSP shall deploy the skilled and qualified manpower for running the Contact Centre.

2. Minimum Manpower Profiles: Manpower deployed by MSP shall comply with the recommended support ratios and minimum qualifications criteria, as mentioned in the tables below, for each contact center facility individually (except for no. of Account Head which shall be as defined below). In case of any deviation from the support ratio in either facility, liquidated damages as mentioned in Volume 1 Section 3.3.1 of this RfP shall be levied. The manpower shall be dedicated to GeM account. GeM shall reserve the right to audit manpower

profiles on an ad-hoc basis.

#	Position	Category	Employer of resources	Support Ratio
1.	Account Head	A1	MSP and, if applicable, Sub-contractor	In case there is no sub-contracting, 1 resource from MSP (as mentioned in Volume 1 Section 8.5.1 of the RfP) In case of sub-contracting, 1 resource from MSP (as mentioned in Volume 1 Section 8.5.1 of the RfP) and 1 resource from each sub-contractor involved
	L0, KNE & Escalations			**Support Ratio** *(w.r.t L0, KNE & Escalations agents/ executives)*
2.	Customer Service Executive/ Agents (L0, KNE & Escalations)	A5	MSP/ Sub-contractor	-
3.	Team Leaders (L0, KNE & Escalations)	A4	MSP/ Sub-contractor	1:15
4.	Delivery Lead (L0, KNEs and Escalations)	A2	MSP/ Sub-contractor	1 resource
5.	Assistant Manager/ Deputy Manager/ Manager – Operations (L0, KNE & Escalations)	A3	MSP/ Sub-contractor	1:60
6.	Assistant Manager/ Deputy Manager/ Manager – Training (L0, KNE & Escalations)	A3	MSP/ Sub-contractor	1:250
7.	Assistant Manager / Deputy Manager/	A3	MSP/ Sub-contractor	1:250

#	Role			
	Manager – Quality (L0, KNE & Escalations)			
8.	Assistant Manager/ Deputy Manager/ Manager – MIS (L0, KNE & Escalations)	A3	MSP/ Sub-contractor	1 resource
9.	Quality Analyst (L0, KNE & Escalations)	A4	MSP/ Sub-contractor	1:30
10.	Trainer (L0, KNE & Escalations)	A4	MSP/ Sub-contractor	1:60
11.	Soft-skill Coach (L0, KNE & Escalations)	A3	MSP/ Sub-contractor	1:100
12.	MIS Analyst (L0, KNE & Escalations)	A4	MSP/ Sub-contractor	1:50
13.	Real-time Analyst (L0 only)	A4	MSP/ Sub-contractor	1:50 *(w.r.t L0 agents/ executives)*
	L1			**Support Ratio** *(w.r.t L1 executives)*
14.	Customer Service Executive (L1)	A4	MSP	-
15.	Team Leaders (L1)	A3	MSP	1:15
16.	Delivery Lead (L1)	A1	MSP	1 resource
17.	Assistant Manager/ Deputy Manager/ Manager – Operations (L1)	A2	MSP	1:60
	L2			**Support Ratio** *(w.r.t L2 executives)*
18.	Customer Service Executive (L2)	A3	MSP	-
19.	Assistant Manager/ Deputy Manager/ Manager – Operations (L2)	A2	MSP	1:60
	L1 & L2			**Support Ratio** *(w.r.t L1 & L2 executives)*

#	Position			
20.	Delivery Lead	A1	MSP	1
21.	Assistant Manager/ Deputy Manager/ Manager – Training & Quality (L1 & L2)	A2	MSP	1:250 *(1 resource already accounted for in Volume 1 Section 8.5.1)*
22.	Assistant Manager/ Deputy Manager/ Manager – MIS (L1 & L2)	A2	MSP	1 resource *(1 resource already accounted for in Volume 1 Section 8.5.1)*
23.	Quality Analyst (L1 & L2)	A4	MSP	1:30
24.	Trainer (L1 & L2)	A4	MSP	1:60
25.	MIS Analyst (L1 & L2)	A4	MSP	1:50

Table 9: Contact centre manpower

#	Position	Minimum Qualification
1.	Account Head	1. Account Head shall be dedicated to GeM 2. Must be a graduate or equivalent 3. Experience of at least 13 years of working across customer services or shared services processes 4. Understanding of large-scale government procurement (preferred) 5. Able to lead, manage and communicate confidently and politely, with large teams 6. Effective problem-solving and decision-making skills with experience of managing clients and delivery of large contact centre related projects
2.	Delivery Lead (L0, KNEs and Escalations)	1. Must be a graduate or equivalent 2. Minimum 10 years of experience at Contact Centre 3. Experience of handling business operations & process delivery for contact centres/ shared services set-up 4. Experience of managing large teams of at least 100-200 associates/FTEs in a similar work set-up 5. Experience working in a B2B environment 6. Experience in managing the customer deliverables, process

		maintenance & improvement, and people management
		7. Understanding of large-scale government procurement (preferred)
3.	Delivery Lead (L1 & L2)	1. Must be a graduate or equivalent with a degree/ diploma in Computer science or IT
		2. Minimum 10 years of experience at Contact Centre
		3. Must possess in-depth knowledge of technical aspects of e-commerce/ procurement platforms
		4. Experience of handling business operations & process delivery for contact centres/ shared services set-up
		5. Experience of managing large teams of at least 100-200 associates/FTEs in a similar work set-up
		6. Experience working in a B2B environment
		7. Experience in managing the customer deliverables, process maintenance & improvement, and people management
		8. Understanding of large-scale government procurement (preferred)
4.	Assistant Manager / Deputy Manager/ Manager – Operations (L0, KNE & Escalations)	1. Assistant Manager/ Deputy Manager/ Manager - Operations - Minimum 6/7/8 years of experience at Contact Centre
		2. Must hold a Bachelor's degree, or higher, in operations, or a related field like engineering or supply chain
		3. Specialized skill set in running large scale production operations in a contact centre environment
		4. Experience in leading and managing large high performance teams of associates/managers
		5. Understanding of Lean and Six Sigma, and a keen interest in and familiarity with technical systems related to contact centres
		6. Deep knowledge in continuous improvement methods such as Kaizen, Lean, DMAIC, etc.
		7. Understanding of large-scale government procurement (not mandatory)
5.	Assistant Manager / Deputy Manager/ Manager – Operations (L1&L2)	1. Assistant Manager/ Deputy Manager/ Manager - Operations - Minimum 6/7/8 years of experience at Contact Centre
		2. Must hold a Bachelor's degree, or higher, in operations, or a

		related field like engineering or supply chain
		3. Specialized skill set in running large scale production operations in a contact centre environment
		4. Experience in leading and managing large high performance teams of associates/managers
		5. Understanding of Lean and Six Sigma, and a keen interest in and familiarity with technical systems related to contact centres
		6. Deep knowledge in continuous improvement methods such as Kaizen, Lean, DMAIC, etc.
		7. Must possess knowledge of technical aspects of e-commerce/ procurement platforms
		8. Understanding of large-scale government procurement (not mandatory)
6.	Assistant Manager / Deputy Manager/ Manager – Training (L0, KNE & Escalations)	1. Assistant Manager/ Deputy Manager/ Manager - Training - Minimum 6/7/8 years of experience at Contact Centre 2. Experienced as Training Manager or L&D Manager, preferably in the e-commerce industry 3. Bachelor's or advanced degree in a relevant field 4. Experience in leading and managing large high performance teams of associates/managers
7.	Assistant Manager / Deputy Manager/ Manager – Quality (L0, KNE & Escalations)	1. Assistant Manager/ Deputy Manager/ Manager - Quality - Minimum 6/7/8 years of experience at Contact Centre 2. Must hold a Bachelor's degree or equivalent 3. Working knowledge of workforce management practices and tools, e.g., scheduling software, quality monitoring software 4. Problem-solving and decision-making skills 5. Demonstrated analytics and root cause analysis skills for process improvement initiatives
8.	Assistant Manager / Deputy Manager/ Manager – Training & Quality (L1 & L2)	1. Assistant Manager/ Deputy Manager/ Manager – Training & Quality - Minimum 6/7/8 years of experience at Contact Centre 2. Must hold a Bachelor's degree or equivalent 3. Experience in leading, and managing large high performance teams and training function 4. Working knowledge of workforce management practices and tools, e.g., scheduling software, quality monitoring

		software
		5. Problem-solving and decision-making skills
		6. Demonstrated analytics and root cause analysis skills for process improvement initiatives
		7. Must possess knowledge of technical aspects of e-commerce/ procurement platforms
9.	Assistant Manager/ Deputy Manager/ Manager – MIS	1. Assistant Manager/ Deputy Manager/ Manager - MIS - Minimum 6/7/8 years of experience at Contact Centre
		2. Must be a graduate/ post graduate degree in any discipline (preferably engineering, commerce, business, or related fields)
		3. Experienced in SQL/ MIS/Advance excel/PowerBI
		4. Strong MS Excel knowledge and Power Point presentation skills
		5. Prior exposure to the Business Intelligence (BI) tools, MS office, and other tools and working with cross-functional teams
10.	Team Leaders (L0, KNE & Escalations)	1. Must be a Graduate or equivalent
		2. Able to speak, read and write in English and any one or more of the languages defined in Volume 1 Section 3.1.7.2 of this RFP
		3. Able to communicate confidently and politely, with good speaking skills
		4. Experience of at least 4 years in a Contact Centre and at least 2 years of experience in the same role
		5. Experience in coaching and developing skills of people
		6. Effective problem-solving and decision-making skills
		7. Understanding of large-scale government procurement (not mandatory)
11.	Team Leaders (L1 & L2)	1. Must be a Graduate or equivalent with a degree/ diploma in Computer Science or IT
		2. Minimum 5 years of experience in Technical Helpdesk
		3. Able to speak, read and write in English and any one or more of the languages defined in Volume 1 Section 3.1.7.2 of this RFP
		4. Able to communicate confidently and politely, with good speaking skills
		5. Experience in coaching and developing skills of people

		6. Effective problem-solving and decision-making skills
		7. Understanding of large-scale government procurement (not mandatory)
12.	Customer Service Agents/ Executives (L0, KNE & Escalations)	1. Must be a Graduate or equivalent
		2. Able to speak, read and write in English and any one or more of the languages defined in Volume 1 Section 3.1.7.2 of this RFP
		3. Able to communicate confidently and politely, with good speaking skills
		4. Experience of at least 6 months in a Contact Centre
13.	Customer Service Executives (L1 & L2)	1. Must be a Graduate or equivalent with a degree/ diploma in Computer Science or IT
		2. Minimum 2 years of experience in Technical Helpdesk
		3. Able to speak, read and write in English and any one or more of the languages defined in Volume 1 Section 3.1.7.2 of this RFP
		4. Able to communicate confidently and politely, with good speaking skills
14.	Quality Analyst (L0, KNE & Escalations)	1. Minimum 4 years of relevant experience at Contact Centre and at least 2 years of experience in the same role
		2. Must be a graduate in any discipline.
		3. Experienced in customer services and International Voice Process
		4. Should possess good knowledge in International Voice QA
		5. Should have the required skills to monitor calls, identify errors and provide necessary feedback/ corrective actions
15.	Quality Analyst (L1 & L2)	1. Minimum 4 years of relevant experience at Contact Centre and at least 2 years of experience in the same role
		2. Must be a graduate in any discipline.
		3. Experienced in customer services and International Voice Process
		4. Should possess good knowledge in International Voice QA
		5. Should have the required skills to monitor calls, identify errors and provide necessary feedback/ corrective actions
		6. Must possess knowledge of technical aspects of e-commerce/ procurement platforms
16.	Trainer (L0, KNE & Escalations)	1. Minimum 4 years of relevant experience at Contact Centre

		and at least 2 years of experience in the same role
		2. Must hold a bachelor's degree in education, communication or business or the equivalent combination of education, training or work experience
		3. Advanced presentation, interpersonal, time management, and organizational skills
		4. Strong training program design experience
		5. Excellent verbal and written communication skills
17.	Trainer (L1 & L2)	2. Minimum 4 years of relevant experience at Contact Centre and at least 2 years of experience in the same role
		3. Must hold a bachelor's degree in engineering, education, communication or business or the equivalent combination of education, training or work experience
		4. Advanced presentation, interpersonal, time management, and organizational skills
		5. Strong training program design experience
		6. Excellent verbal and written communication skills
		7. Must possess knowledge of technical aspects of e-commerce/ procurement platforms
18.	Soft-skill Coach	1. Overall at least 5 years of experience and minimum 2 years of experience as Soft-Skill Trainer at Contact Centre
		2. Must be a graduate or equivalent
		3. Strong communication skills
		4. Strong verbal command over English and any one or more of the languages defined in Volume 1 Section 3.1.7.2 of this RFP
19.	MIS Analyst	1. Minimum 2 years of experience at Contact Centre in MIS role
		2. Must hold a graduate/post graduate degree in any discipline (preferably engineering, commerce, business, or related fields)
		3. Strong MS Excel knowledge and Power Point presentation skills
		4. Prior exposure to the Business Intelligence (BI) tools, MS office, and other tools and working with cross-functional teams
20.	Real-time Analyst (L0)	1. Minimum 2 years of relevant experience at Contact Centre
		2. Must be a graduate or equivalent in any discipline

| | | 3. Effective problem-solving and decision-making skills |
| | | 4. Experience in managing real-time floor operations at contact-center, IVR queue monitoring, etc. |

Table 10: Contact Center Manpower Minimum Qualifications

All above positions, including Customer Service Executive/ agents, are required to go through Versant tests, and minimum passing requirement shall be Versant 5 for Voice and 65 for written Versant. The process should be conducted in a designated place with proper surveillance and camera recordings. Versant Test and other hiring processes shall be auditable by GeM as needed. GeM shall also reserve the right to engage in the hiring process of the contact center resources as deemed necessary by GeM. MSP should deploy best of class professionals to ensure successful operations at the Contact Center and Technical Helpdesk throughout the contract duration. In case a resource deemed fit for the role does not meet any of the minimum qualification defined above, MSP can seek a hiring approval from GeM and deploy the resource once approved by GeM.

1. Considering the nature of the Services, training is an important aspect of the GeM Contact Center. The MSP should provision for imparting proper training in soft skills; call handling, exposure to the related application so as to prepare the customer service executives to answer different types of queries, and on other aspects of Contact Center Services.

2. The MSP should ensure that all the customer service executives are put on actual duty only after providing them proper training on at least the following areas:

#	Training Area	Responsibility
1	Soft Skills	MSP
2	Application(s)	MSP
3	Call Handling procedures	MSP
4	GeM business process related/ scripts	MSP (with support from GeM team) Note: For such training sessions, arrangement of logistics, travel, etc. for the MSP's resources shall be the responsibility of the MSP

Table 11: Contact centre training

MSP shall conduct regular Training Needs Assessment and share monthly training plan for batch trainings and refresher trainings for contact centre resources by 25th of the previous month for GeM's approval. MSP shall also share pre-training and post-training efficacy reports for refresher trainings.

MSP shall prepare a knowledge repository, including training material, call type wise decision trees to support agents in answering queries, etc. GeM shall assist MSP in preparing training material (which can be further customized) for business-related trainings.

3.1.7.5   Provisioning of IT Infrastructure for Contact Centre Operations

MSP shall provision for Dialer and related hardware & network components for running the Contact Centre operations.

1. Call centre application:

   a. The software would maintain complete call history of all calls received at the call centre.

   b. The customer service executive would be capturing all the relevant caller information in this for recording customer communication and the software should be integrated with required GeM applications.

   c. The MSP shall provide GeM with all the data of this application at the time of the end of the Agreement period.

2. Toll-Free Number:

   a. MSP shall provide two toll-free numbers, from two different operators.

   b. Both the numbers should be accessible from anywhere in India and from other network operators also. Customers should be able to dial these toll-free numbers from mobile as well as landline.

   c. MSP shall provide the PRI line(s) to route the toll-free number(s); Sufficient PRI/ SIP lines shall be procured to ensure customer gets access to IVR.

3. Automatic Call Distributor (ACD):

   ACD distributes incoming calls to agents as they are received. It should have at least the following features:

   a. The system should be able to intelligently route the callers to agents based on their availability to take calls on a first come first serve basis and appropriate skillset matched with the type of query of the caller.

   b. Standard features like Call Transfer, Conference, Barge-in, Dialed Number Identification Sequence (DNIS), Automatic Number Identification (ANI), Caller Line Identification, etc.

   c. The system should announce the queue waiting time for the caller before getting attended by an agent.

   d. The system shall support the ability to play customized announcements per queue

as defined by the administration.

4. Other Infrastructure to be provided by MSP includes but is not limited to:

   a. Call barging and recording software

   b. Call centre executives' computers, phone sets and headsets

5. MSP shall ensure the application required at the helpdesk is implemented and working successfully.

6. MSP shall ensure all other infrastructure required for IT helpdesk personnel is complete which includes but is not limited to:

   a. Desktop/laptop

   b. Headsets for helpdesk personnel

   c. Extension/telephone no. for helpdesk

   d. Telephone equipment

7. MSP shall be responsible for all communication to the user in terms of IT helpdesk features/call no. for helpdesk etc. through emails, notices, posters etc.

3.1.7.6   Contact Centre Operations Audit

1. GeM will do a random sample survey of calls on Call Quality as well as be involved in calls without prior notification. For this purpose, administration level permissions to access all sub-systems/ servers to monitor and generate reports including those required for cross-verification of SLAs and related payments will be provided by the MSP.

2. All calls (both inbound and outbound) should be recorded. The call data from the tapes/ voice logger should be archived on to hard disk every 30 days. The data on the hard disk should be stored using such naming conventions that support easy retrieval. These records shall be retained on the hard disk for another 60 days. GeM might require the records to be kept for a longer period of time. Commercials for the same shall be provided by the MSP along with the proposal.

3. If it is observed by GeM that a customer service executive/ team leader has misbehaved with a caller on the telephone, or if a complaint is received against any of the Customer service executive/ team leaders or if his/ her performance is found to be lacking in the opinion of GeM, GeM may instruct the MSP to remove such person from GeM Call Centre. Strict zero tolerance policy is to be implemented.

4. All the tickets on logging shall be assigned a severity of the issue.

5. Helpdesk shall be responsible for coordinating with the concerned vendor in case issues are pertaining to any external entity product/ support like:

   a. Respective OEM team

   b. DC/DR Support Team

   c. Network Provider

   d. End-User Devices support provider

6. Helpdesk shall keep the user informed on various stages of resolution.

7. Even if the call is forwarded to an external entity, coordination between user and external entity would be maintained by the helpdesk along with informing the user of on-call status.

8. Tickets that are not meeting SLAs and which are exceptional in nature (highly critical, wider spread etc.) shall be escalated as per the defined escalation matrix.

9. Helpdesk should comply with SLAs applicable to them as mentioned in Volume 1 Section 8.6 of this RFP. The ticket should be resolved within the defined TAT of the ticket. Non-adherence to SLAs shall lead to the imposition of Liquidated Damages.

10. MSP shall analyze all tickets and provide a root cause analysis report on a periodic basis for all the recurring issues. MSP shall ensure that resolution is provided for these problems by respective business or technical teams/ vendors so as to prevent further issues due to the same cause. The report for the same should be submitted to GeM.

11. MSP shall conduct periodic employee satisfaction surveys on helpdesk and ongoing support. Results of the same shall be shared with GeM.

12. During the ongoing support provided by the MSP, GeM may conduct periodic employee satisfaction surveys. Based on the outcome of the survey GeM may request the MSP to modify or improvise the processes.

13. MSP shall share system-generated reports with GeM. These reports can be verified by the GeM team, or an external party nominated by the competent authority at GeM. MSP shall be responsible for providing access to raw data to GeM or external party nominated by the competent authority at GeM as and when requested to facilitate the verification process. These reports shall include but are not limited to the following:

    a. Tickets, devices & system logs/ security logs (category, severity, and status of call etc.)

b. Tickets escalated

c. SLA compliance/non-compliance report

d. Problem Management

e. In response to the report, MSP needs to provide its capability of managing the IT helpdesk as a part of the approach & methodology. Other key factors to be addressed will be as follows:

    i. MSPs processes for IT helpdesk management

    ii. Key learning from similar previous experience

    iii. Escalation procedure for handling significant issues

    iv. Helpdesk staffing

    v. Citations of managing IT helpdesk for application, infrastructure and other IT service

14. Disaster Recovery and Business Continuity: The MSP shall establish policies and procedures to be used for Call Centre systems in the event of a disaster to protect and ensure the continuation of Call Centre services. Both the call center facilities should be designed in a manner that each of them has the equipment and/or resources to recover to recover the Call Centre business functions affected by the occurrence of a disaster in the other call center.

a. At least 25% of the normal operational status of the impacted call center has to be restored within the first 24 hours of the disaster.

b. Within 3 days from the day of the disaster, the GeM call centre should be operational with 100% operational status.

3.1.7.7 Reporting

1. Suitable reporting software should be available to generate standard report formats to measure/ verify various SLAs, for monitoring the performance of FTEs, IVRS, ACD, etc. MSP has to provide a portal for report viewing by GeM or its designated vendor(s). Reports should also be available as "On-Screen Reports" with the capability of exporting it to any user-defined format such as Word, Excel, PDF, etc. & print and email features. The reports should be configurable to be mailed to a defined mailing list.

2. The MSP and GeM will mutually agree on the format of the reports to be submitted by the MSP to GeM. If GeM requests the MSP to provide customized/ ad-hoc reports, the MSP will

provide customized/ ad-hoc reports at no cost to GeM. The reports that must be provided by the MSP include, but are not limited to, the following

a. Reports based on time period/ location/ office

b. Type of grievances/ queries/ demand/ analysis - overall and location wise

c. Call waiting time

d. Disposal rate through IVRS and FTE

e. Lost calls/ unanswered calls

f. System/ position log on off or breakdowns Call time (Average Talk Time/ Hold Time/ Handle Time)

g. Hourly call details

h. Outbound report (Outbound Call Volume & durations)

i. Complaints pending for more than the defined time period

j. Calls Handled

k. Abandoned Call Rate

l. Delay Before Abandon (Average/ Longest)

m. Staffing related Report

n. Call origination report (from portal or toll free number)

o. SL report (CO, CA, SL, Aband, AHT)

p. Agent performance report

q. CSAT (All channels)

r. FCR/Repeat call report

s. Escalation desk and Social media report

t. Call type report

u. Quality dashboard (Voice, Chat, Email)

v. Training Dashboard (Voice, Chat, Email)

w. TAT adherence report (1st response time, resolution time)

x. SPV pendency Report

y. KPI One view

z. Buyer / Seller view on tickets, CSAT, FCR, SL, Ticket closure

aa. Ticket closure TAT - Call type wise

bb. Capacity planner (All desks)

cc. Bottom Quartile Management (BQM) Process Report

dd. Escalation Desk RCA and Analysis

ee. Repeat call analysis (Voice and non-voice)

ff. DSAT Analysis (Voice and non-voice)

gg. Downtime tracker

hh. Headcount Tracker

ii. Attrition analysis

jj. AHT Analysis

kk. Chat Report

ll. Email Report

mm. Web ticket report

nn. Walk-in desk report

oo. Month on Month, Year on Year KPI view

pp. Hourly/ Half hourly volume analysis (Calls, emails, web, chat and Tickets)

qq. Ageing wise tickets status and pendency

rr. Weekly / Monthly Review deck - Every Friday (Weekly)/ Every 5th of the month

(Monthly)

ss. Performance snap on What's app (same day FTD and next day MTD)

tt. Ticket Reopen report

uu. Other monthly MIS, SLA reports, number of FTEs logged in FTE wise, language wise, etc.

vv. Call type wise reports and Analysis

ww. Quality Reports, as aligned with GeM

xx. Stack Ranking Report Continuous Improvement process to be followed with regular inputs/ updates/ action plans from MSP on process improvements, projects initiated & efficacy reports

yy. Initiatives and Contact Centre meeting review reports

zz. Pre- and post-training efficacy reports

aaa. Any other report as requested by GeM

3.1.7.8 Monitoring

1. A facility should be available for GeM's monitoring team, external & internal auditors to periodically inspect the functioning of the Call Centre.

2. The monitoring team should be able to access all subsystems and records.

3. Additionally, it should be possible to remotely monitor performance on all SLAs/ KPIs and also of all the applications provided by the system i.e., calls in queue, the number of agents logged in, number of agents, abandoned/ answered calls, call types, etc. by designated Call Centre Coordinator or Call Centre in-charge.

As a part of the proposal, the MSP needs to provide a detailed approach for provisioning, running & maintaining GeM Contact Centre Operations as per the requirements specified.

3.1.7.9 CRM for Helpdesk

The CRM solution shall provide for both inbound and outbound channel support with associated technologies as mentioned below:

1. CRM (product) with functionalities including, but not limited to,

a. Assignment of tickets to multiple contact centre departments

b. Monitoring of tickets and ticket journey with reporting of time taken by each department to resolve tickets

c. API functionality to facilitate integrations

d. Reporting of all channels in a single view

e. Functionalities such as restriction of generation of multiple duplicate tickets from single email ID

2. IVR

3. ACD

4. CTI

5. Call logger

6. Quality Management System

7. Email response system

8. Reporting systems

9. Scanning Solution for letters & faxes

The CRM solution should support all the requirements of the Technical Support team. For queries that cannot be answered using a pre-defined script, the query shall be logged in the CRM and tracked to resolution.

The CRM shall provide advanced analytics services to reduce queries & grievances and improve the quality of customer service by the contact centre. Examples include root cause analysis of top 10 queries/ complaints across regions, early detection of issues, number and type of calls by the users in the last 6 months, etc.

The CRM solution shall also measure performance indicators and SLAs for contact centre and contact centre agents. Some examples of the measurements are:

1. Response and Resolution times for grievances

2. Average Handling Time (AHT)

3. IVRS Efficiency

4. First Time Resolution (FTR)

The CRM shall function as "Voice of Customer" to provide GeM with routine feedback on the perception of the quality of services offered by GeM.

Types of queries and grievances: An illustrative list of queries and grievances that may be posted with the GeM Contact Centre is given below to assist the bidder in understanding the nature of support to be provided using the CRM solution.

Queries (Sample)	Grievances (Sample)

General - Queries
1. Seller / Service Provider queries
    a. How do I register as a Seller / Service Provider
    b. What are the benefits of registering into the GeM system
    c. Can I exit from GeM
    d. What documents are required from me to register in the GeM
    e. Do I have to sign an agreement
    f. How I will be paid for my sales
	1. Seller/ Service Provider Grievances
	    a. Payment not received
	    b. Agreement is delayed

2. Buyers Queries
    a. The Buyers' interface module is down.
    b. How do I become a user of GeM System
    c. Change of address and change of destination
	2. Buyers Grievances
	    a. I am not able to register
	    b. How do I determine L1 prices
	    c. How do I look at the bidding capacity of a Bidder?

Table 12: Contact centre queries

3.1.8 Operations and Maintenance

The MSP will operate and maintain all the components of the new GeM platform from the date of Go-Live through the duration of this Agreement. The O&M is divided into the following parts:

3.1.8.1 Application Support and Maintenance

Application support includes, but is not limited to, production monitoring, troubleshooting, and addressing functionality/ availability and performance issues and also implementing system change

requests etc. The MSP shall maintain the application software in good working conditions; and perform changes and upgrades to the applications as requested by the GeM team. All tickets related to any issue/complaint/observation about the system shall be maintained in an ITIL compliant comprehensive ticketing solution. Key activities to be performed by the MSP during the application support phase are as follows:

1. Compliance to SLA

   The MSP shall ensure compliance with SLAs as indicated in Volume 1 Section 8.6 of this RFP, and any upgrades/major changes to the software shall be planned by the MSP while ensuring that the SLA requirements are met at no additional cost to the GeM.

2. Annual Technology Support

   The MSP shall be responsible for arranging annual technology support to the GeM for the OEM products provided by respective OEMs during the entire O&M phase. It is mandatory for the MSP to take enterprise level annual support over the entire Agreement duration at minimum for the software(s) mentioned below:

   a. Operating System

   b. Virtualization layers

   c. RDBMS

   d. Data warehouse

   e. Analytics tool

   f. All third-party products/ engines deployed in the GeM Solution

3. Application Software Maintenance

   The MSP shall provide continuous and indefinite support through on-site team/telephone/E-mail/Video Conferencing/installation visits as required.

   The MSP shall address all the errors/bugs/gaps in the functionalities of the solution (vis- à-vis the FRS, BRD and SRS signed off) at no additional cost during the O&M phase.

   All patches and upgrades from OEMs shall be implemented by the MSP. Technical upgrades of installation to the new version, as and when required, shall be done by the MSP. Any version upgrades of the software/tool/application will be done by the MSP after seeking prior approval from the GeM and submitting the impact assessment of an upgrade as such.

   Any changes/upgrades to the software performed during the support phase shall be subject to comprehensive and integrated testing by the MSP in order to ensure that the changes

implemented in the system meet the specified requirements and do not impact any other existing functions of the system. A detailed process in this regard will be finalized by the MSP in consultation with the GeM.

An Issue log shall be maintained by the MSP for the errors and bugs identified in the solution as well as any changes implemented in the solution and shall be periodically submitted to the GeM team.

The MSP will inform GeM (at least on a monthly basis) about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the MSP shall inform GeM immediately along with any relevant recommendations. The report shall also contain the MSP's recommendations on update/upgrade, benefits, impact analysis etc. The MSP needs to execute updates/upgrades through a formal change management process and subsequently update all documentation and Knowledge databases etc. The MSP will carry out all required updates/upgrades by following defined processes at no additional cost.

4. Problem identification and Resolution:

   a. Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve in turn leading to application hindrances. The MSP shall resolve all the application problems through the implementation of the identified solution (e.g., system malfunctions, performance problems and data corruption etc.) and perform root cause analysis to identify and resolve the root cause as needed. GeM technical team shall reserve the right to sought the root cause analysis pertaining to an issue from MSP for its acceptance and closure.

   b. Monthly reports on problems identified and resolved would be submitted to the GeM team along with recommended solutions.

5. Change and Version Control

   All planned or emergency changes to any component of the system shall be carried out through the approved Change Management process. The MSP needs to follow all such processes (based on industry ITSM framework) at all times. For any change, MSP shall ensure:

   a. Detailed impact analysis is conducted

   b. All Change plans are backed by Rollback plans

   c. Appropriate communication on the change required has taken place

   d. Requisite approvals have been received

   e. Schedules have been adjusted to minimize the impact on the Production

environment

f. All associated documentation is updated post stabilization of the implemented change

g. Version control is maintained for all software changes

The MSP shall define the Software Change Management and Version Control Process. For any changes to the solution, the MSP has to prepare detailed documentation including proposed changes and impact to the system in terms of functional outcomes/additional features added to the system etc. The MSP shall ensure that software and hardware version control is carried out for the entire Agreement duration. MSP shall also provide the facility to make minor changes such as change in bid related information including end date, reference price, etc., with approval from relevant GeM stakeholders, via back-end in case front-end functionality is unavailable to the users

6. Maintain configuration information

The MSP shall maintain version control and configuration information for application software and any relevant system documentation.

7. Training

The MSP shall conduct trainings for the GeM personnel whenever there is any change in the system functionality. All Training plans have to be mutually agreed on with the GeM team. All such trainings will be mandatory and shall not incur any additional cost. Monthly (or fortnightly if required) training sessions need to be conducted by MSP for new features and functionalities. Recording for the same needs to be shared with GeM Project Directors.

8. Maintain System documentation

The MSP shall maintain at least the following minimum documentation, with proper version control, with respect to the GeM system:

a. The high-level design of the whole system

b. Low-level design for whole system/module design level

c. System Requirements Specifications (SRS)

d. Any other explanatory notes about the system

e. Traceability matrix

f. Compilation environment

Access to the repository of all documentation, training recordings, etc. needs to be provided to designated GeM officials as required. The documentation shall be updated periodically to incorporate the changes made to the system/ module and shall be maintained with proper version control. The MSP shall also ensure that any software system documentation is updated with regard to the following:

   a. Source code is documented

   b. Functional specifications are documented

   c. Application documentation is updated to reflect ongoing maintenance and enhancements including FRS and SRS in accordance with the defined standards

   d. User manuals and training manuals   are updated to reflect ongoing changes/enhancements

   e. Standard practices of version control and management are adopted and followed

9. All project documents need to follow a proper version control mechanism. The MSP will be required to keep all project documentation updated and ensure the updated project documents are submitted to the GeM by the end of the next quarter in case of any change.

10. For application support, the MSP shall assign a dedicated software support team to be based at the MSP's location as a single point of contact for the resolution of all application-related issues. This team will receive and resolve all the application related tickets/incidents. In the technical proposal, the MSP needs to provide the proposed application support team structure including the number of team members proposed to be deployed along with the roles and skills of each. The Application Support team shall comprise the MSP's employees.

11. Any software changes required due to errors/problems/bugs/gaps in the developed software/application will not be considered as part of change control and will have to be completed by the MSP at no additional cost   (even if it requires any enhancements/ customizations).

3.1.8.2   Master Data Maintenance

MSP shall be responsible for maintaining all the master data for the platform that would include the following:

1. New products and services

2. New product and service categories

3. Buyer departments

4. Vendors

5. Internal and external users

3.1.8.3   Audits

1. GeM will get the system audited by 3rd party auditors at its own discretion. The MSP shall provide necessary support and co-operation for the audit and close the findings of the audit.

2. GeM to provide advance notice of 2 weeks for any such audit to ensure preparedness and smooth functioning at MSP end.

3. In addition to the audits conducted by GeM at its own discretion, MSP shall follow the audit schedule mentioned in the table below and ensure timely initiation and completion of all periodic audits. Any fee required to be paid to the auditor shall be borne by GeM. All other charges/ costs involved in successful completion of the audits shall be borne by the MSP.

4. GeM will arrange for the ISO 27001 audit to be conducted for the solution. The MSP shall cooperate, provide necessary support, and close the findings of the audit.

First Internal Audit Report	6 months post Go-Live
System audit	Annual
SLA audit report	Every quarter
Application audit	Annual
ISO 27001 audit report	Annual
Asset audit	Annual
ITIL audit	Annual

Table 13: Audit schedule

5. The MSP shall provide an option for online audit option for Auditors (CAG).

6. For STQC audit and all other periodic GeM audits, MSP should support GeM at no extra cost which would include provisioning of all necessary documentation, arrangement of CSP site visits etc.

3.1.9 Advanced Data Analytics and Business Intelligence

MSP shall provision for the capability to analyze large quantities of business data, transform the data into intelligence and insight, and deliver this intelligence and insight to GeM's Buyers, Sellers, and internal users. MSP shall setup an Advanced Data Analytics & Business Intelligence system for GeM to help increase efficiency through the availability of reliable data in a timely manner. MSP shall setup or build an enterprise-wide Data Analytics & BI system covering KPIs from different perspectives such as Division, Function, Process, Buyers and Sellers perspective. System shall also enable high-end data mining and forecasting/ statistical analysis to support Planning & Forecasting, Strategic Planning and Scorecards / Dashboards for GeM System.

The MSP's Scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of an enterprise-level Data Analytics & Business Intelligence Solution for GeM. The MSP shall enable GeM to provide comprehensive procurement monitoring through Business Intelligence (Dashboards and reports) and Analytics. The mechanism would also allow for alerts, reminders, etc. to be sent through a unified dashboard that will let the user control their procurement or supply.

Additionally, MSP shall also implement Advanced Analytics/ AI/ ML related use cases as aligned with GeM during design phase – e.g. procurement planning, product recommendations, product demand forecasting, etc. In addition to this, MSP shall be responsible for implementation of existing use cases currently implemented/ being implemented by GeM or third-party nominated by GeM such as market intelligence gathering (competitive analysis, price benchmarking), duplicate image identification to ensure catalogue accuracy, identification of anomalous behaviour (collusion, cartelization, etc.), bidding analytics (measure health of a bid by assessing participation, Seller offering, L1 price), NLP based search engine.

1. The MSP shall carry out a detailed requirement phase upon award of the contract/ Agreement to review the data analytics requirements for the Advanced Data Analytics module.

2. The MSP shall produce detailed functional specifications and design specifications, including detailing the data analytics module to be developed, system architecture design, design principles/considerations, etc.

3. Regarding the BI system, the MSP shall also perform the following:

    a. Propose, design, and implement an integrated Data Analytics module

    b. Quality assurance test for Data Analytics module

    c. Provide documentation for the Data Analytics module

    d. Perform integration with internal & external systems' data sources for the Data Analytics module

e. Master Data Management for all applications under GeM

f. The solution must have self-service client services such as system and data status dashboards, electronic data dictionaries, and manual data upload

4. The solution must have analytics and dynamic reporting for reporting carried out by GeM. All functions should have their reporting function and allow for exportable formats such as pdf, excel, and others in agreement with GeM.

5. The MSP should propose tools that allow generation of customizable reports. The generation of the reports shall not impair the system performance.

6. Cost for all visualization tools like Tableau/Power BI/Alteryx/QlikSense etc. should be borne by MSP. MSP shall provision for enterprise level licenses of software approved by GeM so that no. of users with access does not become a restriction during the duration of this Agreement.

7. An indicative list of current dashboards and reports have been provided in Volume 1 Section 8.1.16 of this RFP. The final list of dashboards and reports to be developed, along with user access related details, shall be aligned with GeM during the design phase as mentioned in Volume 1 Section 5 of this RFP.

8. The Data Analytics module should allow GeM to customize notification of certain indicators that GeM is interested in to trigger activities/actions. The Data Analytics module should have a user interface to extract data based on the data required for self- analytics and report generation. The Data Analytics module should also allow for ad-hoc queries pertaining to the module for quick access to real-time information and allow users to put in parameters to view the data from different perspectives

9. The MSP would enable GeM to have a complete set of tools to support the entire decision making. These applications will be essential to analyse KPIs in a structured and comprehensive way through a scorecard mechanism so that better choices are made on procurement resource allocation and releasing resources to various Buyers/Departments of the Government of India.

10. MSP has to prepare detailed requirements around reports and also study GeM KPIs to define required reports, analytics capability to meet the GeM business needs.

11. A scheduled (weekly, fortnightly, monthly, quarterly, yearly) report needs to be extracted based on the agreed format and quantum and submitted to the GeM for KPI tracking purposes.

12. GeM or a third party agency (CERT-In empaneled) nominated by GeM shall reserve the right to audit the dashboards and reports created by MSP to ensure data integrity, cyber security, authenticity etc. In such cases, MSP shall provide GeM/ agency nominated by GeM access to all supporting information requested, including raw data, etc. The proposed Data Analytics &

BI Solution for GeM should meet the full and complete functional & technical requirements as provided in Volume 1 Section 8.1 and 8.2 of this RFP respectively.

13. MSP shall ensure that all information, data, documentation, etc. provided by the MSP or its consortium partners (in case of consortium) or sub-contractors to GeM is accurate. In case the information, data, documentation etc. shared is found to be inaccurate, it shall be treated as an event of default and shall be governed by Volume 3 Section 13 of this RFP. In case this inaccurate information/ data/ documentation shared was used to calculate the payout or fee payable/ already paid to the MSP, then GeM reserves the right to re-calculate the payout or fee payable/ paid to the MSP and recover any amount paid previously over and above the re-calculated payout or fees.

3.2 Business Services

This section details GeM's business processes that MSP will be required to perform and facilitate as part of the engagement. The MSP is required to perform all steps necessary to implement the processes as indicated within the Business Architecture section detailed out in the Volume 1 Section 8.1 of this RFP. Please note that this RFP lays down indicative and broad set of process requirements for estimation purposes. Participants will be expected to engage in a detailed requirement gathering and BRD exercise with GeM and final processes will be reviewed and signed by GeM.

3.2.1 Registration

The GeM system provides the registration process for Buyers and Sellers/ Service Providers. These processes have been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.1.1 Buyer Registration & Management

The Buyer Registration & Management process shall include, but is not limited to, the following stages:

Buyer's Registration: In case of Government Buyer Registration, MSP shall facilitate registration of two types of users –Primary Users (or HoDs) and they will create Secondary Users i.e., business users with one or more of the following roles – Buyer, Consignee, Paying Authority/ DDO (Drawing & Disbursement Officer), Technical Evaluator, Indentor

Once registered, the primary user initiates the process of secondary user registration for appropriate roles such as that of procurement officer, consignee, indenter, etc. Secondary users get an invitation link after user addition/activation by primary user. The primary user of the Buyer department also has the functionality to manage (update/ delete) secondary user accounts.

The MSP shall register the Buyer through the Buyer interface portal through secure login mechanism. The MSP shall communicate the acceptance or rejection of a Buyer registration on the GeM portal to the Buyer.

Support for Buyers: The MSP shall aid Buyers for redressal of the grievance by issuing a ticket and resolution of the ticket in a time bound manner through a Customer Relationship Management (CRM) solution. The MSP shall provide regular MIS reports to GeM.

Communication: The MSP shall communicate with the Buyers through SMS, email, Whatsapp, CRM, Contact Centre and any other communication channel that GeM decides to deploy in the future, about the availability of new products on the GeM portal. The MSP shall endeavor to promote the GeM portal in the best possible manner

3.2.1.2 Seller/ Service Provider Registration & Management

The Seller/ Service Provider Registration & Management process shall include, but is not limited to, the following stages:

Seller / Service provider Registration: The MSP shall facilitate the provision for online registration of the Sellers/ Service Providers through the registration panel. Any new Seller/ Service Provider should be able to apply for registration on the registration panel. The Acceptance / Rejection criterions would be defined by GeM and system shall have interlocks to validate these during the time of registration and send an alert of acceptance or rejection. All rejection cases must be accompanied by the reason for rejection. A Seller can reapply when he meets the defined criterions.

Sellers/ Service providers, all of them are required to go through the registration process which primarily includes below three steps:

1. Creation of a primary user ID for Sellers and Service Providers, preferably an authorized person such as Director of the organization or a Key Person/Proprietor

2. Seller or Service Provider profile completion and verification

3. Secondary user creation by the registered primary user of Sellers and Service Providers (optional)

Once a Seller account is closed, Seller is not allowed to create new account in next one year.

Support for Sellers/ Service Providers: The MSP shall aid Sellers/ Service Providers for redressal of the grievance by issuing a ticket and resolution of the ticket in a time bound manner through a Customer Relationship Management (CRM) solution. The MSP shall provide regular MIS reports to GeM.

Communication: The MSP shall communicate with the Sellers/ Service Providers through SMS, email, and CRM contact Centres about the new requirements/registration of new products/ services, on the GeM portal. The MSP shall endeavor to promote the GeM portal in the best possible manner.

Seller Exit Management: The MSP shall also manage the exit of the Seller from the GeM portal.

3.2.1.3 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for registration processes as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create an onboarding manual for the Sellers/ Service Providers and Buyers registration and lifecycle management on GeM portal. The MSP shall continuously update the onboarding manual on a real-time basis with proper version control of the master document

4. The MSP shall create all relevant documentation needed (e.g., BRDs, SOPs, etc.) and shall continuously update the same on a quarterly basis with proper version control of the master document

5. Preparation of draft Seller's/ Buyer's Agreement for onboarding of Seller/ Buyer to be approved by GeM MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.2 Category Management

As a marketplace, one of the founding pillars of GeM is its products and services categories. Given the multitude of government Buyer organizations that transact on GeM and their large procurement needs, the scale, and the spread of type of transactions on the GeM platform is enormous. Currently, unique product and service categories are organized across four classification levels (L1 to L4) as per United Nations Standard Products and Services Code (UNSPSC) classification system. GeM will soon transition towards Indian Trade Classification Harmonized System (ITC-HS), and consequently, modification or addition of further classification levels shall be needed. Category management process involves below stakeholders:

1. Category creator: Establishes new category section, classifies the category hierarchy, and assigns it to a relevant work group in the system

2. Work group:

   a. Category maker: Defines the category configurations and specifications

   b. Category checker: Reviews and approves the category-related details

   c. Catalogue agent: Responsible for transparently reviewing and approving uploaded product/ services catalogue and brands by the relevant Sellers within the category

(from MSP)

The process includes category creation and maintenance. Category creation involves design of Technical Parameters (TP) related to the products or services, List of Values (LoV) corresponding to each TP and other category-related attributes such as ordinal parameters, dependencies between TPs, and TP based rule engines (e.g., higher is better or lower is better), etc. Category maintenance involves regular revision of the TPs, list of values, and category-related features and functionalities in-line with changing demands of Buyers/Sellers, market growth and government policies. It allows category maker and checker to add or modify specifications in an existing category.

The category management process has been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.2.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for category management process as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a *quarterly* basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.3 Catalogue Management

E-catalogues shall contain information about the products and services in the electronic procurement environment. The catalogue management system supports the definition, storage, retrieval, and management of product/ service information throughout the e-procurement process.

Some of the key processes involved in catalogue management are brand creation, catalogue creation, catalogue approval and catalogue upgradation/ modification.

The product/ service catalogues are managed category wise and are divided into product/ service categories, sub-categories, micro categories etc. The basic structure and features of the catalogue would be managed by GeM, however each Seller/ Service Provider, through the Seller's dashboard, will have access to Products/Services catalogues (category-wise) offered by him/ her. The Seller/ Service Provider can also add, delete or modify specifications (e.g., price, quantity, features, etc.) of the products/services offered by him/ her at all times.

Catalogue Management shall include but not limited to the following stages:

Uploading services/ products details including inventory and price: The MSP shall provision a dashboard for the registered Sellers/ Service Providers for uploading the products, services, inventory details (in case of products) and the price of the products/ services.

The system shall allow upload via dashboard, APIs and through bulk sheet.

The MSP shall ensure that the Seller/ Service Provider shall not register and supply products/goods/articles/services which are banned by GeM. The MSP shall obtain such list from GeM and upload on GeM System for Seller/ Service Provider's reference and shall also form a part of Seller/ Service Provider's Agreement. The MSP shall also ensure that the Sellers who are registered on GeM System are authorized to sell and/or promote the products by the OEMs of the products.

Modifying products/ services details: The MSP shall ensure that the dashboard allows the registered Sellers/ Service Providers to modify the products/ services details

Deleting the products/ services: The MSP shall ensure that the dashboard allows the registered Sellers/ Service Providers to delete the product/ service catalogues.

The catalogue management process has been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.3.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for catalogue management process for both products and services, as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.4 E-Procurement

Overall e-procurement process at GeM comprises of various procurement processes via which government Buyers can procure goods/ services and even sell specific items they own:

1. Direct purchase (for orders < INR 25000)

2. Lowest cost purchase (L1 buying) (for orders < INR 5 Lacs)

3. Category-led bid and reverse auction

4. Custom bid (for products/ service unavailable on GeM)

5. Bill of Quantity (to procure multiple products in varying quantities)

6. Demand Aggregation (to pool demand across departments under central/ state ministry)

7. Forward auction

The order value limits mentioned above for direct purchase and lowest cost purchase are subjected to change as per GFR guidelines and hence, must be configurable for GeM to modify as needed.

Apart from the above procurement methods, GeM is developing the functionalities to facilitate procurement via other procurement methods such as push button procurement, bunching of products and services, single packet procurement, etc.

The e-procurement processes have been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.4.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for all e-procurement processes on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.5   Contract Management

Contract Management involves two crucial aspects:

1. **e-Contracting:** e-Contracting makes it easy for Buyers and Sellers/ Service Providers to finalize the terms & conditions and other key aspects of an order placed on GeM. This functionality allows Buyers to create, generate and digitally sign an order/ service contract. GeM system has pre-designed template of contract for each product category. The digitally signed contract is then sent to the Seller/ Service Provider for acceptance. The contract is auto accepted except in cases highlighted in Volume 1 Section 8.1 of this RFP.

2. **Post-contract Management:** This process involves amendments that can be request by

Buyer/ Seller/ Service Provider post a contract has been signed by both parties. These currently include quantity amendment and delivery period amendment for products and quantity, contract period amendments and contract extension for services.

The contract management processes have been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.5.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for all contract management processes on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a *quarterly* basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.6 Order Fulfilment

Once the contract is generated and Seller/ Service Provider has accepted the order on GeM, the Seller/Service Provider is required to process and fulfill the order. GeM and MSP shall ensure facilitation of various sub-processes within Order Fulfilment, some of which are mentioned below:

1. Payment of transaction charges/ Annual Milestone Charges from Seller to GeM

2. Performance Bank Guarantee form submission and verification

3. Invoice generation

4. Submission of proof of delivery

5. PRC and CRAC generation in case of product and SDAC generation in case of services

6. Supplementary invoice generation in case of rejected quantity during PRC/ CRAC

Detailed process flow for order fulfilment process has been provided in Volume 1 Section 8.1 of this RFP.

3.2.6.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for order fulfilment process on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.7 Payments

Outgoing payments or payments from Buyer to Seller/ Service Providers include payments for orders, staggered payments in case of services, etc. To initiate the payment, Buyer first needs to finalize the bill and get it approved by the relevant payment authority (DDO/ PAO) within the Buyer organization. To facilitate payments, GeM offers multiple mechanisms for the Buyer, as mentioned below:

1. PFMS (for Centre)

2. IFMS (for States)

3. GeM Pool Account (GPA) (for Centre, State and PSUs)

4. Online payment via payment gateways: GeM has integration SBI MOPS to facilitate Buyers who are using payment gateways for internet banking, corporate net banking, RTGS and NEFT, etc. (for PSUs)

5. Dedicated integrations with Indian Railways, CGDA, CRPF, MoPR systems for payments

6. ERP based payment systems: The bill data is pushed to Buyer ERP systems, CPSUs pay via their own systems, and shares payment status with GeM (e.g., IOCL, ONGC, SAIL, BHEL, etc.)

Detailed process flows, and system requirements have been provided in Volume 1 Section 8.1 of this RFP.

3.2.7.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for order fulfilment process on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a *quarterly* basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

5. The MSP shall implement all relevant integrations to support the payment process

3.2.8 Receipt of Incoming Payment

This process involves management of incoming payments to GeM from Sellers, Service Providers or Buyers. These include:

1. Caution Money Deposit

2. Transaction Charges and Annual Milestone Charges

3. Interest Charges in case of delayed payments

4. Business Cockpit charges

5. Any other charges/ fees/ EMD/ BG to be collected from Seller/Buyer/ Service Provider basis any ministry order/ notification/ approved board resolution from time to time

6. Online refund of charges in case of applicable situations such as excess charge, double payments, etc.

GeM also supports upload of proofs of security fee deposit (e.g., bank guarantee) by allowing Seller/ Service Providers to upload relevant documents for Buyer's reference to the GeM portal.

The process flows for different types of incoming payments and fee deposits have been detailed in Volume 1 Section 8.1 of this RFP.

3.2.8.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for finance process on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

5. The MSP shall implement all relevant integrations to support the incoming payment process

3.2.9 Incident Management

Any action that is a variation from the terms and conditions of procurement on GeM and relevant Government rules and guidelines is termed as "deviation".

GeM's Incident Management Policy guides the mechanism for reporting and initiating action on any such deviation and elaborates the overall framework for identification and handling of deviations on GeM portal.

An incident can be raised by Buyer, Seller, Service Provider, GeM Admin and automatically via GeM portal as well. There are two types of incidents: pre-contract and post-contract, spanning across multiple categories of severity (mild, serious, severe, grave). Buyer, Seller, Service Provider, GeM Admin can raise an incident via the Incident Management Dashboard. Buyer and Seller/ Service Provider can try to get a resolution mutually within the stipulated time from the party against whom the incident has been raised. In case of no resolution at user end, the incident can be escalated to GeM Admin after completion of the stipulated time. GeM Admin takes suitable action based on available facts and merit of the case.

MSP shall be responsible for immediately notifying GeM about any dispute which comes to its knowledge that has arisen between the Buyer and the Seller/ Service Provider and also for reasonably assisting GeM in managing dispute resolution between Buyer and Seller, at no additional cost to GeM, by providing all available facts, data, documents, reports etc. required for managing the dispute resolution. It is clarified that as part of this obligation, the MSP will not be required to provide any legal advice or legal opinion.

The incident management process flow has been detailed in Volume 1 Section 8.1 of this RFP.

3.2.9.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for incident management process on GeM as detailed in Volume 1 Section 8.1 of this RFP and in accordance with GeM's Incident Management Policy. MSP shall automate the process and implement decision support systems for evaluation of all type of incidents

2. Implementation, management and maintenance of user friendly Incident Management Dashboard

3. Automated reporting systems to be developed by MSP for management reporting on incidents, and related TATs, pendency, etc.

4. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

5. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

6. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.10 Request Management System

Request Management System can be used by various stakeholders to raise requests detailed below.

1. Procedural or policy request

2. Category upgradation (for Buyers, Sellers, and Service Providers)

3. New category creation request (currently under revamp)

RMS provides a systematic way for users to submit their requests for approval/ resolution. Created requests go through the maker-checker concept for implementation in the system and are tracked via a unique reference number. Once the request is resolved, the request initiator is notified via email.

The request management process flow has been detailed in Volume 1 Section 8.1 of this RFP.

3.2.10.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for request management process on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.11 Learning Management System

Learning Management System or LMS is a tool/platform to cater to the training needs of individual stakeholders of GeM be it Buyers, Sellers, or trainers. The platform has complete repository of GeM's training material and features functionalities such as FAQs, certifications, demo portal to practically explore GeM portal, option to provide feedback for training, attendance etc. GeM LMS is an invaluable, user-centric knowledge repository featuring learning paths to meet user specific needs and learn the ecosystem better.

A Buyer or Seller registered on GeM can use his/her credentials to log in to the LMS. Training institutes can also be a part of the LMS portal after their ID and passwords are created, post a request for account creation is raised to GeM.

3.2.11.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of business architecture for learning management system and process on GeM as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. MSP shall update the demo portal monthly to reflect all latest changes introduced on the GeM portal

4. The MSP shall create all relevant documentation (e.g., self-help manuals, training material for different processes and modules, FAQs, audio-visual training content, etc.) needed and shall continuously update the same on a real-time basis with version control of the master document

5. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.12 Trainings

MSP is required to offer offline/ online trainings on the functioning of GeM portal to Buyers, Sellers, Service Providers, etc. at their request. Hence, MSP shall deploy a team of master trainers which shall work under GeM supervision to offer these trainings. GeM shall reserve the right to direct MSP to replace a training related resource in case their performance is not found to be satisfactory.

3.2.12.1 Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Offline/ Online trainings via well-trained master trainers to GeM users (Buyers/ Sellers/ Service Providers). Number of trainers per language to be finalized in mutual alignment with GeM during design phase as mentioned in Volume 1 Section 5 of the RFP.

2. Development and implementation of new functionalities/ interventions required, as mentioned in Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation (e.g., training materials, FAQs, user manuals, etc.) needed and shall continuously update the same on a real-time basis with version control of the master document

3.2.13 Business Facilitation

The MSP is required to have a dedicated team of business facilitators for each state. Business Facilitators will work under the supervision of GeM and help in familiarizing the Buyers with GeM portal and aid the users in case they are facing any issue w.r.t using the GeM portal. GeM shall reserve the right to direct MSP to replace a business facilitation resource in case their performance is not found to be satisfactory. Number of Business Facilitators per language to be finalized in mutual alignment with GeM during design phase as mentioned in Volume 1 Section 5 of the RFP.

3.2.13.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Team of well-trained business facilitators

2. Development and implementation of new functionalities/ interventions required over the course of engagement period

3. The MSP shall create all relevant documentation (e.g., training materials, FAQs, user manuals, etc.) needed and shall continuously update the same on a real-time basis with version control

3.2.14 Inspection and Quality Testing

The MSP's Scope of work includes monitoring & management of Inspection & Quality Testing wherever required. The MSP is required to create a workflow through a dedicated module for Inspection & Quality Testing in the GeM System, so that a time-bound inspection of the products by the Buyer himself or through a third-party on behalf of Buyer and GeM can take place. Buyer may choose to avail the inspection services (Ground-Level inspection services) from their empaneled agencies such as SGS India, TCR engineering, BIS, Rites, etc. In case the Buyer does not have any empaneled agencies, Buyer should have the functionality to be able to procure the inspection services from appropriate Service Provider basis their requirements and budget via GeM. MSP shall be responsible for developing such a process flow.

While creating a product bid, Buyers can avail the option for Inspection for the products being procured via the bid by selecting 'Yes' w.r.t 'Is Inspection Required'. The system will ask them to select their 'Empaneled Agency/ Inspection Authority' (e.g., DGQA, DRDO, EIL, NITRA, etc.) that will be conducting the inspection to ensure that the product conforms to the contractual requirements. Buyers can select their agency and proceed with the bid.

3.2.14.1 Deliverables:

1. The MSP by itself is not required to carry out the Inspection & Quality testing however, MSP has to facilitate, monitor, and manage the Inspection & QA process.

2. The MSP shall update the Inspection Manual, digitize it and upload on the GeM System after due approval from GeM.

3. The MSP shall develop the Inspection and QA Testing Module in the GeM portal and the Mobile App, providing interface for initiating and undertaking the Inspection & QA module

4. Development and implementation of new functionalities/ interventions required over the course of engagement period

5. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

6. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.15 Audit Trail

An Audit Trail is a step-by-step record of any action or transaction performed in the system. An audit trail is important to verify and validate business transactions by tracking selected user activities, event source, and data access used to create or modify a record. More details around this process have been provided in Volume 1 Section 8.1 of this RFP.

3.2.15.1 Deliverables:

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of the audit trail process as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required as per Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the

same on a *quarterly* basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.16 Vendor Rating Assessment

The MSP shall facilitate the vendor rating assessment process (currently deployed for products). An objective methodology has been deployed to calculate Seller rating on GeM using varying weightages for different variables, namely delivery, reliability, quality, users' feedback, and Buyers' feedback. Additionally, the rating calculated is adjusted based on the penalty arising out of reporting of incidents, i.e., the Seller's non-compliance with the terms and conditions agreed between the Seller, Buyer, and the GeM platform. This gives the overall final rating for the Sellers. The MSP shall facilitate the process to capture Buyer and user's feedback on GeM portal with approval of GeM.

The vendor rating methodology has been explained in detail in Volume 1 Section 8.1 of this RFP.

3.2.16.1 Deliverables:

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development and implementation of the vendor rating assessment process as detailed in Volume 1 Section 8.1 of this RFP

2. Development and implementation of new functionalities/ interventions required as per Volume 1 Section 8.1 of this RFP

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

4. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.17 Advanced Analytics & Business Intelligence

GeM provides its internal and external users access to various dashboards and periodic reports. These business intelligence & analytics tools are leveraged to inform decision making processes both within GeM and the Buyer/ Seller/ Service Providers organizations. Additionally, GeM is also implementing multiple AI/ML related use cases to facilitate decision making and augment operations. A summary of these dashboards/ reports has been provided in Volume 1 Section 8.1 of this RFP.

3.2.17.1 Deliverables:

Under this category, the MSP shall specifically deliver the following but not limited to

1. Development, implementation and updation of all relevant dashboards and reports, as detailed in Volume 1 Section 8.1 of this RFP

2. Development, implementation and updation of all existing AI/ML use cases, as detailed in Volume 1 Section 8.1 of this RFP

3. Development and implementation of new use cases/ functionalities/ interventions required as per Volume 1 Section 8.1 of this RFP

4. Issuing and monitoring user access to various dashboards and reports

5. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

6. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.18 Administration

The MSP shall be responsible for end-to-end management of various admin and technical aspects of GeM (e.g., Portal Management, Category Management System, Marketplace Management, etc.). This also includes creating and configuring user and admin roles (e.g., finance, joint director, etc.) and granting them specific privileges from back end to ensure smooth functioning of the processes. A summary of the user roles and role descriptions has been provided in Volume 1 Section 8.1 of this RFP.

3.2.18.1   Deliverables:

Under this category, the MSP shall specifically deliver the following but not limited to

1. Creation, configuration and monitoring of all user/ admin roles as detailed in Volume 1 Section 8.1 of this RFP

2. Implementation and monitoring of system administration processes including but not limited to portal management, category management system, marketplace management, etc.

3. Development and implementation of new functionalities/ interventions required as per Volume 1 Section 8.1 of this RFP

4. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

5. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.19 External Integrations

GeM supports multiple integrations with third parties to support business processes. For instance, GeM has integrations with PFMS, IFMS, banks and payment gateways to support payment processes. Additionally, GeM has multiple lending integrations – GeM Sahay to support working capital requirements of Seller/ Service Providers to fulfill orders and TReDS to provide payment support to Buyers to ensure timely payments to Sellers/ Service Providers.

GeM also has integrations with multiple verification bodies such as UIDAI, ITR services, GST Portal, MCA-21, Udyam, DIPP, etc. to validate information provided by GeM users (Buyer/ Seller/ Service Provider). Apart from these, GeM is also integrated with select Buyer and Seller ERP systems to make information exchange easy.

GeM has been actively looking to expand its third-party integrations (e.g., include more banks, payment gateways, IndiaPost for logistics, etc.) to support additional features on GeM as the platform grows.

3.2.19.1   Deliverables:

Under this category, the MSP shall specifically deliver the following but not limited to, as per alignment with GeM at the time of functional requirement sign-offs:

1. Implementation of all existing and currently ongoing integrations (indicatively defined in Volume 1 Section 8.1 of this RFP). All costs, including one-time as well as per transaction/ recurring costs, pertaining to all integrations (per transaction/ recurring costs wherever applicable - e.g., UIDAI, GSTN, SMS, PAN, WhatsApp, etc.) shall be borne by the MSP.

2. Implementation of additional/ new integrations as required by GeM (defined in Volume 1 Section 8.1 of this RFP)

3. Development and implementation of new functionalities/ interventions required within existing integrations

4. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

5. MSP shall also provide quarterly reports of all changes made/ being made to the module

3.2.20 Marketing and Promotion

The MSP shall be responsible to market & promote the GeM portal among all stakeholders of the GeM ecosystem during the entire project duration. The MSP shall carry out at least the following activities for the same among others:

1. Create an effective Content Marketing & Communication Strategy for different channels (e.g.,

social media, offline mediums, GeM website, other government websites, etc. in alignment with GeM) to engage and attract Buyers / Sellers / other stakeholders for GeM. A proper, omni-channel communication strategy shall be established which typically should include:

a. Branding guidelines including for usage, support, events etc.

b. Reviewing vision and overarching messaging for content design and dissemination.

c. Performance assessment

d. Analysis of metrics for social/digital media such as Reach, Demographic Breakdown in terms of age, profession, etc. Performance of different kinds of content such as bilingual tweets, engagement, etc.

e. A report on media mentions in traditional media including print, radio and television, of key stakeholders of GeM and its various activities. For example, number of articles published, events conducted and highlighted in print or television, etc.

2. Preparation and submission of a clear Annual Marketing & Communication Plan broken down into Quarterly strategy, actual deliverables, person responsible, timeline, financial implication to steer the entire marketing function for the engagement period

3. Quarterly review of marketing plan, marketing expenditure, and performance summary across campaigns and target audience (to be prepared and shared by MSP) with GeM to make necessary adjustments for effective engagement

4. Develop an approach of systematic content creation and updation in the form of blogs/interviews/success stories to cascade the GeM agenda to a wider audience. Target audience has to be finely discussed and decided upon in alignment with GeM

5. Develop & implement automated Email Marketing Campaigns and customized push notifications for Buyers & Sellers / Service Providers separately. The MSP shall also use mailing lists to reach out to the customers with customized messages and communication. The MSP shall broadcast newsletters to keep the prospective customers informed of the sale promotions, new product announcements, new features, etc.

6. Monitor and identify key trending themes, issues, and reputational risks for GeM and work with GeM to address the same

7. Identify and launch new channels according to the engagement pattern analysis of the target audience e.g., Newsletters, WhatsApp bot (in alignment with GeM)

8. Provision for enablement, business development and maintenance of digital banners / video advertisements / e-Mail or SMS marketing campaigns on GeM website. MSP shall configure the website and provide other necessary support to GeM

9. Design the web & mobile optimized website, pages, content and optimize them to generate a steady stream of traffic from SEO, and constantly maintaining & improving SEO in order to be in the top rankings in searches

10. Provide all necessary tools to facilitate marketing & promotion activities including, but not limited to, campaign & content creation and management, performance monitoring, marketing intelligence gathering, etc.

11. Provide the necessary support to GeM during various government events, exhibitions, fairs where GeM may want to deploy a stall/pavilion for marketing & promotions

12. Other Marketing & Promotions activities as decided by GeM from time to time

The MSP is to invest in marketing & promotion activities, as per the approved marketing plan by GeM, keeping in view the overall feasibility and viability of the business. MSP shall have to invest 5% of the total revenue earned by MSP (including fixed and variable payout components as defined in volume 1 Section 6 of this RFP) towards the marketing & promotion activities. MSP shall prepare comprehensive marketing & promotion activities plan and budget as detailed above. This plan needs to consider higher budget allocations in the initial years and subsequently tailor the plan to remain within the overall 5% commitment of the total revenue towards marketing & promotion activities. This plan and budget would require to be approved by GeM from time to time.

The actual amount (as % of total revenue) spent on marketing & promotion activities will be calculated at the end of engagement period. If the amount is less than 5%, GeM will recover the remaining amount from the MSP. If the amount is higher than 5% then GeM will pay back the excess amount to the MSP.

Revenue Sharing from Advertisements on GeM: MSP, either in-house or through an advertisement agency, shall strive to generate additional revenue from advertisements on the GeM website. Advertisement agency, to be onboarded by MSP, shall be approved by GeM. GeM shall define the advertisement policy including guidelines around nature of advertisements that can be published on GeM platform. All the guidelines related to publishing of advertisements on GeM shall be in adherence to GeM's advertisement policy and shall be aligned and approved by GeM. For the same, MSP shall be paid 25% of the net revenue generated from advertisements on GeM i.e., after deduction of payment done to the Advertisement agency. MSP shall make all necessary modifications/developments in the portal for uploading and running these advertisements and shall be responsible for overall management of the Advertisement agency as well. No extra payment shall be made to MSP for these modifications and developments.

3.2.21 Certificate Authority and e-Sign Solution

GeM intends to implement a Certificate Authority and e-sign solution for the purpose of issuing e-sign for GeM users without any dependency on external parties. MSP shall be responsible for the design, supply, installation, commissioning, implementation and support for Certificate Authority solution as per existing and future CCA guidelines.

"e-Sign" service is an online Electronic Signature Service in which the key pair generation, certification of the public key by the Certificate Authority and digital signature creation for electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services.

3.2.21.1   Deliverables

Under this category, the MSP shall specifically deliver the following but not limited to

1. Design, supply, installation, commissioning, implementation and support for Certificate Authority and e-sign solution as mentioned in Volume 1 Section 8.1 of this RFP

2. MSP shall also provision for all infrastructural requirements for the same functionality, with physical separation via air gap, as per guidelines defined by Controller of Certifying Authorities

3. The MSP shall create all relevant documentation needed and shall continuously update the same on a quarterly basis with proper version control of the master document

3.3 Deployment of resources

This section outlines guidelines for staffing and provisioning of manpower for this project. The bidder should study these guidelines carefully and adherence or deviations to any terms should be clearly highlighted in the technical bid submitted.

3.3.1 Guidelines for provisioning of manpower

1. The MSP's operations to be carried out in a hybrid mode, with 50 onsite resources at GeM premises, while the remaining employees at MSP managed facilities, as below:

   a. MSP shall deploy 50 resources onsite at GeM premises, in line with requirement defined in Volume 1 Section 8.5 of this RFP. These 50 resources must include the 14 Key Resources defined in Volume 2 Section 2.3.3 of this RFP. Remaining onsite resources can be mutually agreed between GeM and MSP.

   b. Other named resources in line with Volume 1 Section 8.5 of this RFP shall be deployed offsite by the MSP at MSP managed facilities located in Delhi / NCR region. These resources shall be readily available for in-person discussions with GeM officials, as and when required by GeM, to ensure smooth functioning.

   c. Any additional resources deployed over and above the above mentioned resources can be located anywhere across India. These resources shall be ready to travel for in-person discussions with GeM, as and when required by GeM, to ensure smooth

functioning.

d. The deployment related requirements mentioned above are in addition to, and not in derogation of, the requirements mentioned in Volume 1 Section 3.1.7 of this RFP, and the two are to be read harmoniously.

2. The MSP shall provide a resource deployment plan, along with location, as part of detailed Project Plan submission phase as defined in Volume 1 Section 5 of this RFP.

3. The resource deployment plan should also include an organization chart showing the proposed organization to be established by the MSP for the execution of the scope of work. The organization chart should clearly bring out variations to the organization structure if any envisaged by the MSP for various phases/stages of the project.

4. A separate organization structure should be provided for clearly identifiable activities such as technology services, business services, etc.

5. Detailed CVs should be provided for the 14 key profiles/ roles that are subject to evaluation as per Volume 2 Section 2.3.3 of the RfP. The area of expertise, role and tasks assigned should be clearly identified for each of the key profiles.

6. Key roles in the MSP's team should be held only by permanent employees of the MSP or those on the permanent rolls of the Sub-contractor.

7. The experience and expertise of the human resource held by the MSP or by the Subcontractor who is to be allocated for the key roles/positions is a significant component of MSP evaluation. GeM would interact with the said resources and this interaction shall be considered in evaluations.

8. Additionally, MSP shall deploy, either themselves or basis GeM's directive, any additional resources needed to meet the implementation schedule (Volume 1 Section 5 of this RFP) and SLAs (Volume 1 Section 8.6 of this RFP), over and above the resources mentioned in the resource deployment plan submitted by the MSP. No additional payment shall be made by GeM for these additional resources.

9. MSP shall adhere to the minimum resources requirements specified in Volume 1 Section 8.5.1 and Volume 1 Section 3.1.7.2 of the RFP, as well as the contact center support ratios defined in Volume 1 Section 3.1.7.4 of the RFP for each contact center facility. MSP shall submit the resource deployment plan for each quarter one month prior to the start of the quarter. GeM shall review and approve the workforce and skill sets requirement proposed by MSP (including the minimum manpower requirements mentioned in Volume 1 Section 8.5.1 of this RFP) for each quarter to ensure right set of skillsets are available for achieving the platform vision for the future. For contact center and technical helpdesk resources, a monthly capacity plan shall be submitted by the MSP as per Volume 1 Section 3.1.7.2 of the RFP.

10. MSP understands that non-deployment of any manpower resources as detailed in clause (9) above, shall cause loss to GeM and hamper the smooth functioning of the services. Hence, in case of non-deployment of any resource or deviation from the minimum resource requirements or support ratios defined in this RFP and revisions approved by GeM to the same in subsequent quarters, MSP shall be liable for Liquidated Damages (over and above the 20% upper cap for Liquidated Damages defined in Volume 1 Section 8.6), under following categories of resources, as defined below:

    a. For contact center resources defined in Volume 1 Section 3.1.7.2 and Volume 1 3.1.7.4 of the RfP

        i. Category A1 resources: 0.065% of Annual Fixed O&M Fee per resource per calendar month

        ii. Category A2 resources: 0.045% of Annual Fixed O&M Fee per resource per calendar month

        iii. Category A3 resources: 0.03% of Annual Fixed O&M Fee per resource per calendar month

        iv. Category A4 resources: 0.02% of Annual Fixed O&M Fee per resource per calendar month

        v. Category A5 resources: 0.015% of Annual Fixed O&M Fee per resource per calendar month

    b. For minimum resource requirements defined in Volume 1 Section 8.5.1 of the RfP

        i. Category C1 resources: 0.15% of Annual Fixed O&M Fee per resource per calendar month

        ii. Category C2 resources: 0.1% of Annual Fixed O&M Fee per resource per calendar month

        iii. Category C3 resources: 0.075% of Annual Fixed O&M Fee per resource per calendar month

If a resource is not deployed for a period of less than or more than a month then the liquidated damages shall be calculated on a pro-rata basis. These amounts shall increase every year at a rate of 6% to account for inflation. These liquidated damages shall be calculated on monthly basis and reported quarterly in adherence with the measurement and reporting methodology of other SLAs.

11. The MSP's obligation to render its services onsite (from GeM's Premises) or offsite (from MSP manages facilities) shall be subject to any applicable government restrictions that may be

imposed by any government authorities by way of any government orders/notifications/circulars or any other mode for reasons such as prevention of outbreak of pandemic etc. On occasion of any such government restrictions which may directly or indirectly hinder in rendering of services at the physical location of GeM, GeM shall allow the MSP to render its services from remote location for such period till the government restrictions are waived off by any further government orders/notifications/circulars.

3.3.2 Competency requirements of the MSP's team and sub-contracted teams

1. The MSP shall provide and deploy only those manpower resources who are qualified/skilled and experienced in their respective trades and who are competent to deliver in a proper and timely manner (in line with requirements of this RFP).

2. The MSP shall ensure that the teams are competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Agreement. The MSP shall ensure that due diligence of such personnel deployed on the project including satisfactory background checks are completed. Documentary evidence for such background checks would need to be made available to GeM or their authorized representatives, whenever required.

3. The MSP shall ensure that the Services are performed through the efforts of the MSP's Team, in accordance with the terms hereof and to the satisfaction of GeM.

3.3.3 Replacement of Personnel

1. The MSP should to the best of its efforts, avoid any change in the organization structure proposed for execution of the scope of services or replacement of any manpower resource.

2. If the same is however unavoidable, due to circumstances such as the resource leaving the MSP's organization or the sub-contracted agency's organization etc., MSP shall immediately inform GeM in writing and atleast 30 (thirty) days prior to resource's leaving the project.

3. If any resource is absent or going to be absent for a period of more than 30 (thirty) days, MSP shall promptly notify the same to the Purchaser and the resource shall be replaced by the MSP, unless otherwise directed by GeM.

4. MSP understands that replacement of any manpower resource proposed by the MSP as per requirements defined in Volume 1 Section 8.5 of this RFP shall cause loss to GeM and hamper the smooth functioning of the services. Hence, in case of replacement of any manpower resource (except all Contact Center and Technical Helpdesk resources defined in Section 3.1.7.2, 3.1.7.4 and 8.5.1), MSP shall be liable for Liquidated Damages (over and above the 20% upper cap for Liquidated Damages defined in Volume 1 Section 8.6), under following 3

(three) categories of resources, as defined below:

c. **Category C1 resources:** 0.4% of Annual Fixed O&M fee (as defined in Volume 1 Section 6 of this RFP) per resource replaced

d. **Category C2 resources**: 0.2% of Annual Fixed O&M fee (as defined in Volume 1 Section 6 of this RFP) per resource replaced

e. **Category C3 resources:** 0.1% of Annual Fixed O&M fee (as defined in Volume 1 Section 6 of this RFP) per resource replaced

5. The 14 Key Resources mentioned in Volume 2 Section 2.3.3 shall be deployed by the MSP immediately on this project within timelines defined in Volume 1 Section 8.6 of this RFP.

   a. If at the time of mobilization of Key Resources (T+21 days), GeM finds that any of the 14 Key Resources are replaced on or after the date of Technical Presentation by the MSP, as mentioned in Volume 2 Section 2.3.2 of the RFP, until date of signing of Agreement, MSP shall be liable for 4% of Annual Fixed O&M fee (as defined in Volume 1 Section 6 of this RFP) per resource replaced as liquidated damages. However, these liquidated damages will not be levied in case there is a delay in finalization of the Agreement beyond the original Bid Validity period of 120 days.

   b. If any of these 14 Key Resources are replaced within the first 2 years of the duration of the Agreement, MSP shall be liable for 4% of Annual Fixed O&M fee (as defined in Volume 1 Section 6 of this RFP) per resource replaced as liquidated damages. These Liquidated Damages shall be over and above the 20% upper cap for Liquidated Damages defined in Volume 1 Section 8.6 of this RFP. After 2 years, normal resource replacement Liquidated Damage clause, as mentioned above in Volume 1 Section 3.3.3. clause (4) of the RFP, shall be applicable basis the category of each resources as defined in Volume 1 Section 8.5 of this RFP.

6. MSP shall replace the resource with a better or equally competent resource within 30 days (extendable up to a total of 60 days with the consent of GeM) of the resource's resignation/ absence/ termination. In case MSP fails to replace the resource within 30 days or the agreed timelines, the following Liquidated Damages (in addition to LD defined in Clause (4) and (5) above), shall be levied basis delay over and above the 30 days or agreed timelines:

   a. Delay of <10 days: 0.01% of Annual Fixed O&M fee per resource

   b. Delay of 10-20 days: 0.02% of Annual Fixed O&M fee per resource

   c. Delay of >20 days: 0.002% of Annual Fixed O&M fee for each day delayed per resource

Replacement delay LD is applicable to all resources including contact center & technical

helpdesk resources.

7. Liquidated Damages as defined above shall not be applicable in case of replacement of resource is due to approved leaves by the MSP and GeM on account of maternity leave, paternity leave, serious medical conditions/ ailments certified by a reputed medical practitioner and approved by GeM, and demise of the resource.

8. In case of replacement of any manpower resource, the MSP should ensure efficient knowledge transfer from the outgoing resource to the incoming resource at the earliest, adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service.

3.3.4   Removal of Personnel

1. GeM's representative may at any time object to and require the MSP to remove forthwith from the Project Site any authorized representative or employee of the MSP or any person(s) of the MSP's team, if, in the opinion of GeM's Representative the person in question has misconducted or his/her deployment is otherwise considered undesirable by GeM's Representative. The MSP shall forthwith remove and shall not again deploy the person without the written consent of GeM's Representative.

2. GeM's Representative may at any time object to and request the MSP to remove from the Sites any of MSP's authorized representative including any employee of the MSP or his team or any person(s) deployed by MSP or his team for professional incompetence or negligence or for being deployed for work for which he is not suited.

3. GeM's Representative shall state to the MSP in writing his reasons for any request or requirement pursuant to this clause. The MSP shall replace every person removed, pursuant to this section, with a competent substitute within 30 days of removal (extendable up to a total of 60 days with the consent of GeM), and at no extra cost to GeM.

4. All manpower resources deployed by the MSP for the execution of this Agreement must strictly adhere to the attendance reporting procedures and make their services available for the entire reporting time period at respective Sites, GeM's Office or any other location designated by GeM.

5. MSP shall maintain internal timesheets that shall be submitted on a monthly basis to GeM.

6. All manpower resources deployed by the MSP for the execution of this Agreement shall follow GeM's holiday calendar throughout the duration of this Agreement. All profiles should comply with 100% attendance requirement excluding holidays, leaves, etc.

3.3.5 Logistics requirements of the Personnel

1. The MSP shall be responsible for the deployment, transportation, accommodation, and other requirements of all its employees required for the execution of the work and provision of services for all costs/charges in connection thereof and no liability in this regard shall be attached to the Purchaser.

2. MSP should be able to provide all kinds of infrastructure and arrangements to enable the remote working of employees if a situation may arise to necessitate the same, ensuring adequate cyber security and data protection measures or any other instructions issued by the Purchaser

3.3.6 Personnel requirement benchmarking

1. MSP shall submit the resource deployment plan for each quarter one month prior to the start of the quarter. GeM shall review and approve the workforce and skill sets requirement proposed by MSP (including the minimum manpower requirements mentioned in Volume 1 Section 8.5.1 of this RFP) for each quarter to ensure right set of skillsets are available for achieving the platform vision for the future. For contact center and technical helpdesk resources, a monthly capacity plan shall be submitted by the MSP as per Volume 1 Section 3.1.7.2 of the RFP. Any commercial implication for the same will need to be discussed and agreed upon mutually.

3.3.7 Escalation Matrix

1. As part of the technical proposal, the bidder shall provide a detailed Escalation Matrix mapping back to the MSP's organizational structure proposed.

2. The Escalation Matrix should address key requirements stated in the Service Level Agreements for various service delivery activities and cover all major service delivery activities.

3. The triggers for escalation should be clearly identified and stated for each category of service in the Technical Proposal.

3.3.8 Facilities MSP shall provide to its staff

1. The infrastructure including, but not limited to, network/ internet connectivity, or other facilities required for the efficient execution of work under the Agreement, apart from the facilities promised by GeM, should be provided by MSP or its Sub-Contractors to its employees who are working under this Agreement.

2. At a minimum, the MSP shall provide the following facilities to the staff members deployed.

   a. Laptops, Mouse, Modems, mobile phones and other necessary accessories subject to conformance to GeM's security policies

   b. Laptop Maintenance and Troubleshooting Service

   c. Access Card System

   d. Daily consumables such as stationery, notebooks, etc.

3.3.9 Team Composition, Manpower Qualification & Experience Requirements

The team proposed by MSP should have clearly defined staff position across the following categories as defined in Volume 1 Section 8.5 of this RFP.

1. Program Management & Governance

2. Business Services Unit (BSU)

3. Technical Services Unit (TSU)

4. Contract Management Unit

3.3.9.1 Program Management & Governance

In the Program Management & Governance Unit, the MSP is expected to create a Program Management & Governance layer in the organization positioned for the delivery of GeM Solution.

1. The resource deployment plan must mandatorily contain the time commitment of the Sr Director/Vertical head/ relevant CxO/equivalent of the Lead Bidder.

2. The bidder should budget adequate time of senior management of all the sub-contractors proposed and such staff should be available for onsite interactions if required by GeM.

3. The Program Director, Program Managers & team leaders proposed for this project shall be deployed on a full-time basis.

4. Their time commitment should be clearly specified in the resource deployment plan.

3.3.9.2 Business Services Unit (BSU)

The Business Layer of the MSP team shall have multiple teams mapped to different functions as enlisted this RFP. The MSP is expected to study the Scope of Work carefully and size the team accordingly. Minimum number of full-time resources have been specified for Business Services Unit (BSU) in Volume 1 Section 8.5 of this RFP which the MSP has to deploy on the project.

However, the MSP is expected to provide adequate experienced & qualified manpower for each category of resources in order to carry out the work specified in this RFP while meeting the SLA requirements.

3.3.9.3 Technical Services Unit (TSU)

The Technical Layer of the MSP team shall have multiple teams mapped to different functions as enlisted in this RFP. The MSP is expected to study the Scope of Work carefully and size the team accordingly. Minimum number of full-time resources have been specified for Technical Services Unit (TSU) in Volume 1 Section 8.5 of this RFP which the MSP has to deploy on the project. However, the MSP is expected to provide adequate experienced & qualified manpower for each category of resources in order to carry out the work specified in this RFP while meeting the SLA requirements.

3.3.9.4 Contract Management Unit

The Contract Management Unit of the MSP shall have resources for Contract Administration, and all legal matters pertaining to legal terms & conditions for the GeM entity as specified in Volume 3 of this RFP. The MSP is expected to study the Scope of Work carefully and size the team accordingly.

3.3.9.5 Manpower Qualification & Experience Requirement

The MSP has to deploy well qualified and experienced resources having in-depth knowledge & experience of the position for which they are deployed. The resources shall have to carry out work in order to meet the desired objectives of implementing and running the GeM System.

A bare minimum qualification and experience requirements of the resources to be deployed, are given in Volume 1 Section 8.5 of this RFP, along with the indicative high-level roles & responsibilities

of the resources which they are expected to carry out objectively while meeting the SLA requirements.

3.4 Project Management & Governance

3.4.1 Planning and Scheduling

The MSP shall prepare a detailed project plan and get it approved from GeM at the start of the project and ensure it is updated on a monthly basis. The milestone dates have been provided in Volume 1 Section 5 of this RFP. The MSP may suggest changes in project dates without altering the end dates of each activity.

3.4.2 MSP's Programme of Work and Staff Deployment

1. The MSP's programme of work should be synchronized with the resource deployment plan proposed.

2. Within 60 calendar days after the release of Letter of Award under this Contract or prior to kick-off meeting whichever is earlier, the MSP shall submit to GeM for its approval a detailed programme showing the sequence, procedure, and method in which it proposes to carry out the work as stipulated in this RFP, and shall, whenever reasonably required by GeM's Representative, furnish in writing the arrangements and methods proposed to be made for carrying out the work.

3. The programme so submitted by the MSP shall conform to the requirements and timelines specified in the Terms of Reference.

4. GeM and the MSP shall discuss and agree upon the work procedures to be followed for effective execution of the works, which the MSP intends to deploy and shall be clearly specified.

5. Approval by GeM Representative of a programme shall not relieve the MSP of any of his duties or responsibilities under the Contract.

6. However, if the MSP's work plans necessitate a disruption/shutdown in GeM's operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum.

Any time and cost arising due to failure of the MSP to develop/adhere to such a work plan shall be to his account.

3.4.3 Governance, Methodology and Reporting

3.4.3.1 Introduction

This section describes the governance model that will be used throughout the Agreement Term. A distinction is made between two types of governance bodies:

1. Running the programme; and

2. Advising the programme

3.4.3.2 Forum Structure and Representation

Each Party confirms that it intends to co-operate with the other Party and any other party as reasonably requested by the GeM in the performance of its respective obligations under this Agreement and to develop and sustain a mutually beneficial long-term relationship with the other Party.

For the "Joint Design Authority", the Chairperson (or its nominee) will be responsible for:

1. ensuring the proper business and IT representatives (with the necessary delegation) are actively part of the forum;

2. ensuring alignment with other programs in the GeM;

3. act as a final "decision-maker" in case of conflicts and disagreement in the meeting;

4. chairing the meeting;

5. review and sign-off decisions and recommendation;

6. escalate decision to SteerCo (for final approval or recommendation) and present at SteerCo as necessary (with support from the Joint Design Authority as necessary).

For the "Joint Design Authority" an MSP person (or its nominee) shall be nominated and responsible for:

1. scheduling the meetings in accordance with the relevant frequency;

2. setting the meeting agenda and circulating such agenda to all attendees in advance of such meeting (including pre-read materials as necessary);

3. operational management and co-ordination of the material preparation and support to the GeM Chairperson;

4. monitoring the progress of any follow-up tasks or activities agreed to be carried out during the meetings; ensuring that the minutes for the meetings are recorded and disseminated electronically to the appropriate persons and to all meeting participants within 1 (one) Business Day of the meeting;

5. seeking approval of the minutes from the previous meeting at the start of each meeting;

6. and facilitating the process or procedure by which any decision agreed at any meeting is given effect in the appropriate manner.

Without prejudice to the other provisions of the Agreement, each Party shall use its reasonable endeavors to ensure that the membership of each Forum remains stable throughout the Agreement Term. The MSP may provide feedback on any member of the Forum to GeM. GeM may request the MSP to add or replace any of the MSP member(s) of a Forum, and the parties shall meet within 7 (seven) days of the GeM's request to discuss and review such request and agree. Agreed corrective actions (including replacement if still reasonably required) to be implemented within 10 (ten) days from the joint meeting.

Each Party shall ensure that the relevant members for each Forum shall attend the meetings at which that member's attendance is required. If any member is not able to attend a meeting, such member shall ensure that: a delegate who is properly briefed and empowered with no less authority than the absent member attends the relevant meeting, and he or she is debriefed by such delegate after the meeting.

If any member is not able to attend a meeting and is unable to procure the attendance of a delegate at the relevant meeting, the Party that appointed such member shall notify the other Party of such non-attendance giving at least 3 (three) days' notices prior to the meeting.

Forum meetings shall be quorate as long as at least one representative from each party is present unless the additional representation is otherwise required by the GeM.

The Parties shall ensure, as far as reasonably practicable, that all Forums shall as soon as reasonably practicable address the matters raised and resolve Disputes in order to achieve the objectives placed before them. Each Party shall ensure that Forum members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.

Notwithstanding any other provision of this Agreement, the fact that a matter has been exclusively or non-exclusively reserved to a specific Forum for consideration or resolution shall not prevent either Party from being entitled to exercise its rights under this Agreement in its own capacity.

3.4.3.3 Running the program

Multiple governance bodies are required as an integral part of the programme and are responsible for running the programme.

The below chart describes the organizational structure of the Digital and IT Programme:

SteerCo: Overarching steering body:

1. Single scorecard & target across transformation & separation

2. Single budget with clear allocations

3. Prioritization of resource

Transformation Management Office (TMO): Single roadmap and execution across all streams and leads:

1. Single program roadmap & milestones

2. Single comms narrative across all activities

Detailed descriptions of Joint MSP and GeM Forums are set out later in this section.

By the Effective Date, the MSP shall collaborate with GeM to help them establish or use the existing programme governance Forums (as applicable) set out below.

The following table describes indicative governance Forums that need to be scheduled during the Agreement Term. Any additional forum required for the successful delivery of the Services will be agreed upon between the Parties from time to time. The Parties agree to review and adjust, as appropriate, the below Governance bodies following the final Go-Live Milestone in order that the Governance forums then are aligned to the provision of the Run Services. The MSP is free to suggest a different/better governance structure. GeM will be free to choose amongst the governance structure proposed here versus the one proposed by MSP.

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
Steering Committee (SteerCo)	1. Monitor and ensure global progress for a programme (time, budget etc.) 2. Make decisions relevant for global programme	**GeM** 1. GeM CEO /CHRO/CTO/CFO 2. Nominees appointed by GeM CEO	Monthly (unless otherwise stipulated)	As appointed by GeM CEO

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
	3. Identify dependencies with other programs and businesses and take required actions 4. Seek to resolve escalated items from other Programme Forums 5. Seek to resolve disputes between GeM and MSP 6. Set and direct joint protocols to promote healthy ways of working and behaviours 7. Confirm acceptance of Milestone(s) 8. Review and sign off the Stage-Gate as per defined criteria	**MSP** 1. MSP Project Director Nominees appointed by MSP in mutual agreement with GeM		
Programme Management Board	1. Monitor the Implementation Plan 2. Monitor progress and status of the Programme 3. Review and refine Programme plan 4. Manage interdependencies between the GeM, MSP and other third parties that the MSP is dependent upon 5. Monitor the Change	**GeM** 1. Nominees appointed by GeM CEO **MSP** 1. Nominees appointed by MSP in mutual agreement with GeM	Weekly	As appointed by GeM CEO

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
	Control Procedure 6. Resolve issues / conflicts or raise issues / conflicts 7. Manage risks and RAIDs			
Cross-functional workshop	1. Discussion on status updates per workstream, function and region 2. Operational planning and alignment on key interdependencies	**GeM :** 1. Nominees appointed by GeM CEO **MSP(s)** 1. MSP Project Director 2. MSP Technical Program Manager 3. Nominees appointed by MSP in mutual agreement with GeM	As and when required	As appointed by GeM CEO
Quarterly Service and Finance Review Board	1. Review the performance of both Parties against their respective obligations as described in this Agreement; 2. Be responsible for the GeM satisfaction scores, both monthly and annual; 3. Authorize the commissioning and initiation of new development projects;	**GeM** 1. Nominees appointed by GeM CEO **MSP** 1. Nominees appointed by MSP in mutual agreement with GeM	Quarterly	As appointed by GeM CEO

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
	4. Review the MSP's performance of Service as compared against the Agreement provisions; 5. Consider and resolve issues (including commercial issues) and disputes /escalations, as agreed by representatives of both Parties; 6. Ensure the operational service delivers agreed Services and minimizes the risk of a service interruption affecting core business functions. 7. Report on payment and invoicing status 8. Monitor resources ramp-up / ramp-down 9. Coordinate contractual changes and work 10. Monitor and confirm SLAs, KPIs status			
Weekly Service Review	1. Review weekly service performance that includes, Incidents, Problems and proposed	**GeM** 1. Nominees appointed by GeM CEO	1. Weekly	

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
	Changes 2. Ensure the operational service delivers agreed Services and minimizes the risk of service interruption	**MSP** 1. Nominees appointed by MSP in mutual agreement with GeM		

<p align="center">**Table 14: Governance structure**</p>

Other Meetings: Upon request by GeM, the MSP shall participate in programme wide governance meetings with other third-party MSPs. Closer to Go-Live, Daily stand-ups may be set up as requested by GeM.

3.4.3.4 Advising the program

Additionally, the following two governing body Forums, with indicative structures as detailed below, will be established to play an advisory role in the program:

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
Joint Design Authority	1. Provide a joint business & IT forum to assess technology options and make recommendations /decisions 2. Review/Assess Decision items and Change Requests 3. Ensure tech design recommendations/decisions are in accordance with common principles and consistent 4. Interpret business	**GeM** 1. Nominees appointed by GeM CEO **MSP** 1. Nominees appointed by MSP in mutual agreement with GeM 2.	Quarterly	GeM Joint Design Authority Chair

Governance body Forums	Role	Members	Frequency of meetings	Chair-person
	requirements into the need for common services 5. Ensure that recommendations/solutions meet GeM objectives, are cost-effective and are in line with the latest budget 6. Confirm acceptance of Deliverable(s) 7. Review acceptance of Milestone(s) (where required)			
Quarterly delivery reviews/lessons learned	1. Review lessons learned, agree on improvements for ways of working 2. Review and agree on improvement on delivery processes 3. Confirm priorities for the next period	1. Nominees appointed by GeM CEO 2. Nominees appointed by MSP in mutual agreement with GeM	Quarterly	GeM Programme Director

Table 15: Governing body forums

3.4.3.5   Reporting Obligations

With respect to the reporting obligations, the MSP shall:

1. provide to the GeM all reports listed in this section below

2. deliver all the reports as per format, content and frequency defined in this section

3. distribute the reports only to pre-defined distribution lists that will be agreed with the GeM during the project mobilization;

4. consider all reports as Intellectual Property Rights of the GeM hence treating all information as confidential;

5. modify and update the format, content, frequency as requested or agreed by GeM .

6. deliver all reports that are legally required and necessary to satisfy audit and/or regulatory obligations and requirements;

7. in situations where the MSP report requires inputs from external third parties (e.g., other MSPs, or Service Providers), the MSP shall coordinate with the additional third party to request (and follow up as necessary) the provision of the required material in a timely fashion and shall update the GeM of the status of such requests; and

3.4.3.6   Additions, Deletions, Upgrades and Changes

1. Additions, deletions, upgrades, or other changes to the reports shall be subject to the agreement with GeM. On a quarterly basis, the MSP shall review with GeM the list of reports to identify any changes to reporting requirements. Changes to existing reports and the selection of additional reports shall be subject to the agreement provided at no cost where additional reports are part of continuous improvement to and natural growth of the GeM. The MSP shall deliver all reports to the GeM within a mutually agreed timeframe.

2. For changes to reporting that are not part of continuous improvement to or natural growth of the GeM and require additional tooling, the MSP will present a business case for the change in the reporting. Any new reporting as suggested by the MSP in its business case presentation shall not be implemented unless it has been approved in accordance with the Change Control Procedure.

3.4.3.7   Report Structures

1. The MSP shall provide the following type of reports under the Agreement:

    a. Regular progress reports: detailing the advancement of the delivery activities against the Implementation Plan.

    b. Financial and governance reports: detailing the progress of spending against the agreed budget and providing a summary view and forecast of specific governance topics (e.g., invoicing, payments, resourcing status, contractual changes etc.).

    c. Summary programme reports: summarizing on a regular basis the overall progress inclusive of financial indicators, the status of Change Requests (through the Change Control Procedure as set out in Volume 1 Section 8.7 of this RFP) and architectural decisions.

2. For all the mentioned reports the MSP will propose a template format during project mobilization that will be agreed with the GeM.

3. The MSP shall provide the reports in respect of content, frequency, format and audience described in the table below for the Implementation phase:

Report	Frequency	Content	Format	Audience
Progress Status Report	Weekly	Describe the overall progress of the programme in the past week including: **Programme Status** 1. Overall status of the programme (e.g., RAG) including key activities in progress and main achievement 2. Escalations and items for management attention 3. Description of key issues and resolution actions 4. Description of key risks and mitigating actions 5. Status of the programme against baseline schedule with analysis of the variances 6. Key deliverables completed in the period 7. Upcoming milestones 8. Update on critical path and status against the Implementation Plan 9. Dependencies, incl. third party dependencies 10. Forward-looking view of deliverables, milestones, progress against the programme plan **Detailed status by workstream** For each ongoing workstream	Jira or equivalent software or PPT/PDF as aligned with GeM	Programme Management Board Steerco

Report	Frequency	Content	Format	Audience
		(e.g., scrum team in the design phase, rollout team during implementation) a detailed report including 1. Detailed work plan and progress against the baseline 2. Overall status of the workstream including key achievement, activities in progress, outlook on escalation items 3. Forward-looking view of the workstream progress and plan 4. Key risks and issues 5. Key dependencies and roadblocks		
Financial and Governance report	Monthly	A detailed status report providing a clear explanation of the contractual situation, with an outlook on the future events and milestones. The report must include: 1. Upcoming payment milestones and status of the deliverables associated 2. Proposed or agreed contract change notes and relevant status (e.g., new, in progress, signed) 3. Resourcing position of the vendor and outlook on the following 3 months (new resources joining, leaving etc.) 4. Status of Change Requests 5. Status of catalogue orders	Electronic (PPT/ PDF)	Finance Review Board

Report	Frequency	Content	Format	Audience
Summary programme reports	As per Steerco frequency	Detailed programme status illustrating the overall progress of the work including: 1. Key achievements 2. Key activities in progress 3. Status against the baselined plan, critical path and outlook for the following period 4. Steerco escalations and asks 5. Key risk and issues (for Steerco) 6. Outlook for the following period 7. Deep dive on critical workstreams (e.g., design, rollout etc.) 8. Report of decisions for SteerCo approval 9. Summary of stage-gate and milestone completion criteria 10. Summary status of Change Requests 11. Summary of Change Requests for approval	Electronic (PPT / PDF)	Steerco

Table 16: Reports in the implementation phase

4. Additional reports required for auditing, regulatory obligation or programme quality assurance will be needed on an ad-hoc basis and previous agreement with the GeM . For the avoidance of doubt these reports must be provided by the MSP in a reasonable time and free of charge.

5. The MSP shall provide the reports during the O&M Service as per content, frequency, format, and audience described in the table below:

Report	Contents	Input To	Frequency	Provided By

S1 and Major Incident Report	Incident Report Information Management Summary Root Cause	Service Reviews	Occurrence of P1 incidents	MSP Service Delivery Manager (on-shore/off-shore)
Incident/ Request Summary Report	Source of Incident/request Opening group Resolving group Response time Resolution time Current status	Demand Planning	Weekly	MSP Functional Leads
Proactive Problem Management and Incident Trend Analysis	Assessment of recent Incident records for underlying trends that can indicate system issues The output of tools/analysers to predict ticket intake L1 shift-left recommendations	Continuous Improvement and Innovation activities	Monthly	MSP Functional Leads
Service Level Performance Report	Critical SLA status Trend analysis Service status and related credits Issues/risks	GeM Satisfaction Survey Engagement Status Report	Quarterly	MSP Service Delivery Manager (on-shore/off-shore)

Table 17: Reports in O&M phase

3.5 Exit Management & Transition

3.5.1 Purpose

1. This Section sets out the provisions, which will apply on expiry or termination of the Master Service Agreement (Agreement), the Project Implementation, Operation and Management SLA.

2. GeM shall serve notice in writing on the MSP at least 6 months prior to expiry of the Agreement, the Project Implementation, Operation and Management SLA, requiring MSP to initiate the Exit Management and transition process as detailed in this section.

3. In the case of termination of the Master Services Agreement, either of the entire scope of work of the Agreement or of any specific activity under the scope of Agreement, GeM shall instruct

the MSP as to manner and time period of the Exit Management and transition process as detailed in this section.

4. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

3.5.2   Transfer of Assets

1. GeM may serve notice in writing on the MSP at any time during the Exit Management period requiring the MSP and/or its subcontractors to provide GeM with a complete and up to date list of all the Assets.

2. GeM may also serve notice in writing on the MSP at least 30 days prior to the end of the Exit Management period requiring the MSP to sell the Assets, if any, to be transferred to GeM or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

3. In case of Agreement being terminated by GeM, GeM reserves the right to ask MSP to continue running the project operations for a period of 6 months after termination orders are issued.

4. Upon service of a notice under this Article the following provisions shall apply:

    a. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the MSP, the MSP shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to GeM.

    b. All risk in and title to the Assets to be transferred/ to be purchased by GeM pursuant to this Article shall be transferred to GeM, before the last day of the Exit Management period.

    c. GeM shall pay to the MSP such sum representing the Net Block as of the last day of the Exit Management period, (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred post inspection and verification of condition of the asset.

    d. Payment to the outgoing MSP shall be made to the tune of the last set of completed services/deliverables, subject to deduction as per the RFP/ Masters Services Agreement.

    e. The outgoing MSP will pass on to GeM and/or to the Incoming MSP, the subsisting rights in any leased properties/ licensed products on terms not less favorable to GeM/ Incoming MSP, than that enjoyed by the outgoing MSP.

3.5.3 Cooperation and Provision of Information

During the Exit Management period:

The MSP will allow GeM or its nominated agency access to the information reasonably required to define the then-current mode of operation associated with the provision of the services to enable GeM to assess the existing services being delivered; promptly on reasonable request by GeM, the MSP shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the MSP or sub-contractors appointed by the MSP). GeM shall be entitled to a copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The MSP shall permit GeM or its nominated agencies to have reasonable access to its employees and facilities as reasonably required by the Chairperson, Project Implementation Unit, as appointed by GeM CEO to understand the methods of delivery of the services employed by the MSP and to assist appropriate knowledge transfer.

3.5.4 Confidential Information, Security and Data

1. The MSP will promptly on the commencement of the Exit Management period supply to GeM or its nominated agency the following:

    a. information relating to the current Services rendered and customer and performance data relating to the performance of sub-contractors in relation to the Services;

    b. documentation relating to Project's Intellectual Property Rights;

    c. documentation relating to sub-contractors;

    d. all current and updated data as is reasonably required for purposes of GeM or its nominated agencies transitioning the services to its Incoming MSP in a readily available format nominated by GeM, its nominated agency;

    e. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable GeM or its nominated agencies, or its Incoming MSP to carry out due diligence in order to transition the provision of the Services to GeM or its nominated agencies, or its Incoming MSP (as the case may be).

2. Before the expiry of the Exit Management period, the MSP shall deliver to GeM or its nominated agency all-new or updated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the MSP shall be permitted to retain one copy of such materials for legal / compliance / regulatory purposes only with the permission

of GeM.

3. Before the expiry of the Exit Management period, unless otherwise provided under the Agreement, GeM or its nominated agency shall deliver to the MSP all forms of MSP confidential information, which is in the possession or control of Chairperson, Project Implementation Unit, as nominated by GeM CEO or its users.

3.5.5   Employees

1. Promptly on reasonable request at any time during the Exit Management period, the MSP shall, subject to applicable laws, restraints and regulations (including, in particular, those relating to privacy) provide to GeM or its nominated agency a list of all employees (with job titles) of the MSP dedicated to providing the services at the commencement of the Exit Management period.

2. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the MSP to GeM or its nominated agency, or an Incoming MSP ("Transfer Regulation") applies to any or all of the employees of the MSP, then the Parties shall comply with their respective obligations under such Transfer Regulations.

3.5.6   Transfer of Certain Agreements

On request by GeM or its nominated agency the MSP shall effect such assignments, transfers, licenses and sub-licenses as the Chairperson, Project Implementation Unit, as nominated by GeM CEO may require in favor of the Chairperson, Project Implementation Unit, as nominated by GeM CEO or its Incoming MSP in relation to any equipment lease, maintenance or service provision agreement between MSP and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by GeM or its nominated agency or its Incoming MSP.

3.5.7 Rights of Access to Premises

1. At any time during the Exit Management period, where Assets are located at the MSP's premises, the MSP shall be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) GeM or its nominated agency and/or any Incoming MSP in order to make an inventory of the Assets.

2. The MSP shall also give GeM or its nominated agency or its nominated agencies, or any Incoming MSP right of reasonable access to the Implementation Partner's premises and shall procure GeM or its nominated agency or its nominated agencies and any Incoming MSP rights of access to relevant third-party premises during the Exit Management period and for such period of time following termination or expiry of the Agreement as is reasonably necessary to migrate the services to GeM or its nominated agency, or an Incoming MSP.

3.5.8 General Obligations of the MSP

1. The MSP shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to GeM or its nominated agency or its Incoming MSP and which the MSP has in its possession or control at any time during the Exit Management period.

2. For the purposes of this Schedule, anything in the possession or control of any MSP, associated entity, or subcontractor is deemed to be in the possession or control of the MSP.

3. The MSP shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

3.5.9 Exit Management Plan

1. The MSP shall provide GeM or its nominated agency with a recommended Exit Management plan ("Exit Management Plan") within 90 days from effective date of the Agreement, which shall deal with at least the following aspects of Exit Management in relation to the Agreement as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

    a. A detailed program of the transfer process that could be used in conjunction with an Incoming MSP including details of the means to be used to ensure the continuing provision of the Services throughout the transfer process or until the cessation of the Services and of the management structure to be used during the transfer;

    b. plans for the communication with such of the MSP's subcontractors, staff, contractors, customers and any related third party as are necessary to avoid any material detrimental impact on GeM's operations as a result of undertaking the

transfer;

c. (if applicable) proposed arrangements for the segregation of the MSP's networks from the networks employed by GeM and identification of specific security tasks necessary at termination;

d. Plans for the provision of contingent support to GeM, and Incoming MSP for a reasonable period after the transfer.

2. The MSP shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

3. Each Exit Management Plan shall be presented by the MSP to and approved by GeM or its nominated agencies.

4. The terms of payment as stated in the Terms of Payment Schedule include the costs of the MSP complying with its obligations under this Schedule.

5. In the event of termination or expiry of Agreement, and Project Implementation, each Party shall comply with the Exit Management Plan.

6. During the Exit Management period, the MSP shall use its best efforts to deliver the Services.

7. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

8. This Exit Management Plan shall be furnished in writing to GeM or its nominated agencies within 90 days from the Effective Date of Agreement.

3.6 Takeover and Transition of existing GeM system

The purpose of this section is to provide the broad Transition Framework within which the MSP would be required to operate, define the MSP's scope of work and the roles and responsibilities of different stakeholders during various transitions from existing GeM System. The purpose of transition is to

1. Enable MSP to take over existing contracts and be the single vendor for managing various services

2. Enable a well-planned smooth taker over of responsibilities from existing vendor

3. Help GeM control the levels and performance of services through a single vendor

4. Help minimizing the planned down time of services from GeM

3.6.1 Defining Transition Framework

The overall transition of GeM marketplace will follow the structure mentioned in the figure below-
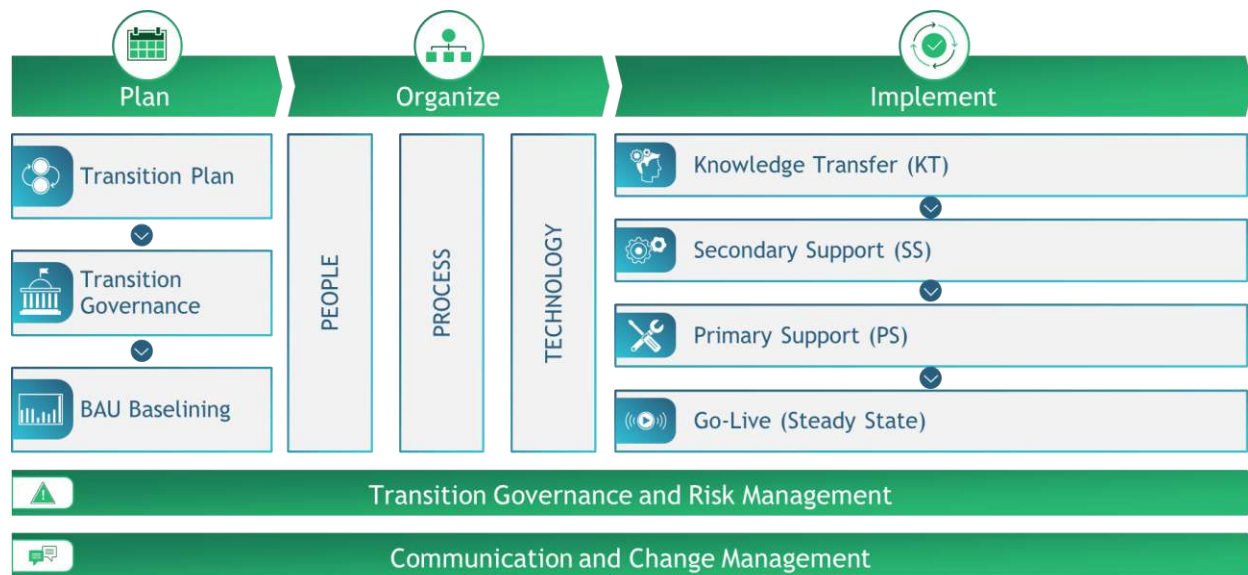
Figure 4: Transition Framework

The objective of this section is to define generic guidelines about transition methodology for the MSP for effective management of the transition of responsibilities. It is expected that all transition activities shall follow a three-phase approach which will include:

1. Pre-transition phase

2. Organize

3. Implement

The three phases will be governed by overall transition governance & risk management guidelines and communication & change management processes.

3.6.1.1   Plan:

The objective of the planning phase is to develop a unified program plan with a detailed transition plan. This phase establishes the transition governance model and processes. Key activities included in the planning phase are as mentioned below-

1. Co-create a program plan with the Purchaser encompassing all relevant work streams– transition, communication, incumbent exit, etc.

2. Create a project plan for transition planning phase encompassing transition plan build, transition governance institutionalization

3. Work with the key stakeholders to establish governance framework in order to initiate transition

4. From the due diligence phase, initiate development of BAU baseline report

3.6.1.2 Organize:

The objective of the organization phase is to institutionalize transition governance framework & implement structure. It ensures the mobilization of people, process, and technology to ensure transition readiness. Key activities included in the organization phase are as mentioned below-

1. Finalize transition governance framework and structure with the Purchaser. Purchaser to assign resources per the governance structure

2. Finalize transition governance processes and templates. Conduct a dry-run on the processes and templates for applicability

3. SP to provide resource ramp-up plan during transition with supporting details.

4. On-boarding check-lists to be prepared and SME calendar to be established

3.6.1.3 Implement:

The objective of the implementation phase is to ensure effectiveness in the transition by enabling knowledge transfer. It ensures organizational and timely communication on transition along with complete primary and secondary support for migration. Key activities included in the implementation phase are as mentioned below-

1. Formulate acceptance criteria and pre-requisites/cut-over plans for each phase of transition. Seek agreement among stakeholders

2. Review service levels and evaluate effectiveness of transition through service level performance

3. Ensure appropriate and timely communications to various organizational groups on status of transition and set expectations on performance levels

4. Sign-off on various gate checks and document for audit trial

3.6.2   Key deliverables

The table below mentions the key deliverables expected in every phase of the transition process-

Phase	Deliverable	Description
Plan	Unified Program Plan	This is the master project plan that would comprise all individual work stream plans. e.g., communication plan, incumbent termination plan, leasing plan, etc.
	Transition Planning Project Plan	Project plan to ensure tracking and closure of transition planning phase. This would detail activities around the detailed transition plan to be built, BAU baseline document, and transition governance
	Detailed Transition Plan	This is the execution level plan that would use to track actual status of transition. Must be as detailed as possible with dependencies clearly accounted. Any scope outside services transition scope that impacts transition should be included as part of this plan
	Transition Plan Dependencies	This document lists overall dependencies of the transition plan apart from inter-dependencies called out in the transition plan. Mostly a contractual document. Also referred to as RAID (Risk, Assumptions, Issues, Dependencies)
	BAU Baseline Document	Laundry list of all BAU activities with RACI defined. To be baselined during transition commencement and contents added/modified as an outcome of KT
	Transition Governance Pack	This document includes 1. Governance framework and model 2. Governance structure 3. RACI matrix 4. Meeting cadence 5. Forums roles responsibilities 6. Reporting cadence 7. Issue escalation and resolution process 8. Change request process 9. On-boarding/Off-boarding process 10. Associated templates/trackers

Phase	Deliverable	Description
Organize	KT Approach Document	The document specifies guidelines for approach towards KT across various locations, the deliverables expected from the exercise and the list of key contacts/owners responsible for KT at each location.
	KT Sessions Tracker	The document contains an operational checklist of perquisites and outcomes of the KT session with regards to agenda, key personnel involved, and handover of documents, if any, etc.
	KT playback and Understanding Document	This document is continuously updated and captures the incoming vendor's understanding of the existing IT environment based on the KT sessions conducted with the exiting vendor
	Asset Tagging process	The document serves as the procedural manual for asset tagging teams across various locations for asset tagging and reconciliation process
	Asset Tagging template	The document serves as the reporting template for compiling the overall progress made in the Asset tagging exercise across all Purchaser locations in scope
	Availability Tracker	The document contains planned absence/vacation of relevant team members
	SME Calendar	This is an extract of the KT plan mapped with the availability of SMEs (incoming as well as outgoing vendor) in order to plan KT sessions
	Knowledge Repository Design	The document contains a broad-level folder structure on Purchaser shared drive with read-access provided to all stakeholders
	Resource Mobilization Checklist	The document contains a ramp-up/ramp-down plan for supplier resources at various Purchaser/MSP locations and helps the Purchaser plan logistics etc.
	Resource On boarding Tracker	The document serves as a location specific checklist for on boarding of supplier resources at various Purchaser/ MSP locations
	ODC Plan	The plan contains detailed list of activities for setting up an Offshore Delivery Center (or a Command Center) at incoming vendor's premises which shall be dedicated solely for serving Purchaser IT operations

Phase	Deliverable	Description
Implement	KT plan	This is the schedule of Knowledge Transition sessions as agreed by the exiting vendor. The schedule cover detailed topics to be covered under each KT session
	KT playback and Understanding Document	This document is continuously updated and captures the incoming vendor's understanding of the existing IT environment based on the KT sessions conducted with the exiting vendor
	KT document charter	This is the list of all key documents the incoming vendor would like to read to understand the running of 'as-is' business operations by the exiting vendor (e.g., policy manuals, SOPs, escalation matrices etc.)
	KT Acceptance Criteria	This is checklist of all key considerations that the Purchaser would like to verify before asking the incoming vendor to start providing shadow support (e.g., documents charter status, status of KT plan etc.)
	SS Approach	The document captures the methodology and plan for providing shadow support, identifies key resource groups and highlights support required from exiting vendor and the Purchaser (e.g., logistics related support, read access to applications, network devices etc.)
	SS Pre-requisites checklist/Cut over plan	The checklist covers the list of requirements that need to be fulfilled at the start of the SS phase for incoming vendor to commence shadow support, e.g., End user notification, Windows login access, read access to systems etc.
	SS Acceptance Criteria	The checklist covers all key considerations that the Purchaser would like to establish before the handover of primary support to incoming vendor under the supervision of the exiting vendor, e.g., SOP, understanding document, shift schedule for PS, list of users and accesses, escalation matrices etc.
	PS Pre-requisites checklist	The checklist covers the list of requirements that need to be fulfilled at the start of the PS phase for incoming vendor to takeover primary support of Purchaser IT operations, e.g., Handover of password/login for administrator access
	PS Acceptance Criteria	The checklist covers all key considerations that the Purchaser would like to verify before the incoming vendor takes over end-to-end responsibility of the 'as-is' IT operations, e.g., completion of all open points related to SS phase, availability

Phase	Deliverable	Description
		of all information related to in-flight projects, gap identification, understanding of reporting requirements, end user communication for handover, etc.
	Solution document	The document covers the scope of services and the methodology (e.g., policy manuals, SOPs) for running Purchaser's IT environment. The document, based on the solution to this RFP, evolves with the key learning captured during the transition phase and is refined based on updated requirements, and volumes. Ideally, the document is submitted by the incoming vendor while takeover of complete responsibility for IT operations
DC Migration	Applications Interface Checklist	The checklist outlines the different interfaces between applications/modules that need to be tested during UAT for functionality and data flow. Critical due to multi-party engagement, multiple geographies and time zones
	Applications Cut-over plan	This is a highly detailed minute-by-minute project plan outlining the activities and the respective owners against specified timelines during migration of applications to new datacenter. The plan also covers interface validation, UAT and discussions for go-ahead for release of application to end users
	Migration planning checklist	This is an operational checklist for execution of the plan. This includes the shift roster of resources supporting during the cutover period, key points of contact, escalation matrix in case of issues, communication cadence, setup of War Room etc.
	Migration controls and evidence collation cadence	This document serves as a reference for the different migration execution teams to collate and save key artifacts at the completion of each activity in the cutover plan for future audit/reference purposes
	Migration communication	The plan serves as a notification to end users ahead of the cutover period regarding the scheduled downtime windows. Once the migration is complete and Go-live is achieved, the users are communicated that the applications are accessible and configuration changes, if any, are notified

Table 18: Key Deliverables

4.   Roles & Responsibilities of the Purchaser

During project duration, GeM shall have the following roles and responsibilities:

1. GeM will provide basic office amenities to the MSP's personnel at its office locations for performing their part of the obligations as outlined in Volume 1 Section 3.3.1 of the RFP.

2. All the facilities provided by GeM are promised to be available only for the time period as agreed upon by MSP and GeM as the official work time and workdays. Beyond the time frame contractually agreed upon, MSP is not entitled to any of these facilities.

3. GeM will provide the following infrastructure and no other facilities beyond this scope mentioned.

    a. Office space for MSP's onsite deployed resources during any shift including Seating Facility that includes desks and chairs for this number of staff.

    b. Server Room & Communication Room for Connectivity from GeM CSP.

    c. LAN connectivity, Network printing facility, Electrical Connectivity

4. Coordination between all the divisions/departments for providing necessary information for the study and development/customization of the necessary solution.

5. Provide necessary support with MSP for conducting workshops for the Stakeholder departments.

6. Monitoring of overall timelines, SLAs, and calculation of Liquidated Damages accordingly.

7. Conducting UAT for the application solution deployed.

8. Issuing the Acceptance Certificate on successful deployment of the software application and for other components of the Scope of Work (wherever required).

9. Any other requirements that could arise during operations for effective governance and to meet any administrative requirement.

10. Ensuring the staff members and other stakeholders attend the training programs as per the schedule defined by GeM.

11. Provide sign off on the deliverables of the project within defined timelines. If GeM fails to intimate acceptance of the deliverables or its objections or feedback to MSP within a period of 30 (thirty) working days from receipt of the deliverable, the deliverable will be considered to be accepted by GeM.

5.   Implementation Schedule

This section outlines the key timelines for new platform development and implementation for the MSP. It draws reference to the Scope of Work outlined in this RFP. All days specified in this section, unless explicitly mentioned, refer to calendar days. T shall be defined as the date of execution/ signing of Agreement between GeM and the MSP. This is to be noted that list of activities / tasks defined in below implementation schedule provide board outline and details shall be finalized by MSP in mutual agreement with GeM. Key milestones specified here shall form the basis for Implementation phase SLAs as defined in Volume 1 Section 8.6 of this RFP. There are a total of 9 milestones in the implementation schedule. Release of payment pertaining to each milestone, as applicable, is subject to successful completion of all activities/ tasks pertaining to that milestone as detailed in the table below.

All "days" mentioned in Volume 1 Section 5 of this RFP are calendar days, unless otherwise specified.

#	Activity/Task for each Milestone	Timeline	Fixed Platform development fee applicable
1.	a. Mobilization and deployment of Key Resources *(as provided during Technical Evaluation and defined in Volume 2 Section 2.3.3 of this RFP)* for requirement gathering, upfront solutioning, project planning, etc.	T+ 21 days	N/A
2.	a. Submission of a detailed implementation Project Plan including design, core development, and acceptance testing phases and resource deployment plan. This shall be reviewed and approved by GeM. b. Submission of a Project Charter incl. Risk Management and Mitigation plan, Information Security Plan, Communication Plan, Data Migration plan, and Change Management Plan, Project Status Reporting & Communication Framework. The Project Charter shall be reviewed and approved by GeM. c. Report on total number of identified & aligned system design documents, test cases to be implemented during the development and implementation phase	T+ 60 days	N/A
3.	a. Onboarding & formation of Agile squads for creation of detailed system architecture and documentation such as BRD, FRS, SRS, HLD, LLD for new tools / new services / new platform *(in compliance with this RFP and in line with the agreed project plan)* b. Finalized and GeM approved list of New business	T+ 3 months	Yes

#	Activity/Task for each Milestone	Timeline	Fixed Platform development fee applicable
	enhancements over and above the existing GeM system, *(in line with the agreed project plan)*		
4.	a. Business design workshops, preparation, and submission documents such as BRD, FRS, SRS, HLD, and LLD *(in compliance with this RFP and in line with the agreed project plan)* b. Submission of Technology & Architecture diagram with cloud and infra provisioning document for new services c. Cloud & infra provisioning of the required services *(in compliance with this RFP and in line with the agreed project plan)*	T+ 6 months	Yes
5.	a. Development, testing, and implementation of 4-5 GeM business modules *(in line with the agreed project plan)* b. Submission of testing and implementation documents with GeM approval *(in line with the agreed project plan)*	T+ 9 months	Yes
	c. Onboarding of teams for Technical Helpdesk, Contact Centre Operations, Business Facilitation, and Training *(Onboarding kick-off to be done 6 months prior to date of current MSP's contract expiry[1] with select resources and systems (Team B and resources defined in Volume 1 Section 3.1.7.2); Ramp up & transition to be done in a phased manner between 6 months prior to date of current MSP's contract expiry and date of complete take over of maintenance and operations of existing GeM platform by incoming MSP as defined below)*	6 months prior to date of current MSP's contract expiry[1]	
6.	a. Completion of knowledge transfer for GeM current system and documentation signoff *(in line with the agreed project plan)* b. MSP to take over and lead the existing GeM platform for maintenance and enhancements, current MSP to support *(in line with the agreed project plan)*	3 months prior to date of current MSP's	Yes

#	Activity/Task for each Milestone	Timeline	Fixed Platform development fee applicable
		contract expiry[1]	
	c. Development, testing, and implementation of 4-5 GeM business modules (in line with the agreed project plan d. Submission of testing and implementation documents with GeM approval (in line with the agreed project plan)	T+12 months	
7.	a. MSP to completely take over the maintenance and operations of existing GeM platform; Current MSP to be relieved as per schedule	As per date of current MSP's contract expiry[1]	Yes
	b. Development, testing, and implementation of 4-5 GeM business modules (in line with the agreed project plan c. Submission of testing and implementation documents with GeM approval (in line with the agreed project plan)	T+15 months	
8.	a. Development, testing, and implementation of 4-5 GeM business modules *(in line with the agreed project plan* b. Submission of testing and implementation documents with GeM approval *(in line with the agreed project plan)* c. Completion of development, testing & implementation of all business modules / services *(in compliance with this RFP and in line with the agreed project plan)* d. All documentation sign-off and approved from GeM (*in line with the agreed project plan*)	T+ 18 months	Yes

#	Activity/Task for each Milestone	Timeline	Fixed Platform development fee applicable
9.	a. Data migration and cutover of transactions into the new GeM platform (*in line with the agreed project plan*) b. Pilot phase launch to test features in final deployment instance (*in line with the agreed project plan*) c. New Platform fully Go–live with all the criteria completed and adhered *(in compliance with this RFP and in line with the agreed project plan)* d. Existing GeM platform phased out	T+ 21 months	Yes

1. Current MSP's contract expiring on 31 December 2023.

Table 19: Implementation Schedule

6. Commercial Conditions

6.1.1 Financial Model for MSP

Since its inception GeM has grown significantly by transforming legacy procurement systems via its disruptive marketplace model. Total GMV (including Goods and Services Tax) on GeM has grown by more than 200% CAGR between FY 2016-17 to FY 2021-22, as highlighted below:

Financial Year	Total GMV (INR Cr.) *(including Goods and Services Tax)*	Total Actual GMV with order value below INR 5 Lakh *(including Goods and Services Tax)*	Total Actual GMV with order value above INR 5 Lakh *(including Goods and Services Tax)*
FY 16-17	422	45	377
FY 17-18	5,876	1,201	4,675
FY 18-19	17,462	4,155	13,307
FY 19-20	22,989	7,491	15,498
FY 20-21	38,577	10,306	28,270
FY 21-22	1,06,699	15,655	91,044
FY 22-23 *(till 15 Sep'22)*	69,005 *(expected for full year: ~2 Lakh)*	6,863	62,142

Table 20: Year-wise GMV growth for GeM

In FY 2021-22, approximately 33.2 Lakh number of orders or transactions happened through GeM platform. Approximately 15% and 180% growth in Buyer and Sellers onboarding was witnessed compared to FY 2020-21, as highlighted below:

Financial Year	No. of Transactions or orders	No. of transactions with value <= INR 5 Lakh	No. of transactions with value > INR 5 Lakh	No. of Buyers transacted	No. of Sellers transacted
FY 16-17	6,284	5,045	1,239	1,200	530
FY 17-18	3,72,734	3,56,901	15,723	20,841	10,432

FY 18-19	13,33,867	12,92,846	41,021	42,916	28,672
FY 19-20	21,81,628	21,44,774	36,854	59,233	42,735
FY 20-21	25,75,108	25,19,911	55,197	74,984	64,684
FY 21-22	33,16,624	31,77,747	1,38,877	1,01,266	1,00,163
FY 22-23 *(till 15 Sep'22)*	16,43,838	15,63,455	80,338	-	-

Table 21: Year-wise platform performance for GeM

Additionally, GeM also hosts a total of over 10,000 categories and nearly 30 Lakhs catalogues across products and services on its platform as of 2021-22, as shown below:

Financial Year	No. of Categories			No. of Catalogues		
	Product	Services	Overall	Product	Services	Overall
FY 16-17	189	-	189	-	829	829
FY 17-18	1,140	2	1,142	3,196	5,157	8,353
FY 18-19	3,142	67	3,209	63,341	34,640	97,981
FY 19-20	5,605	118	5,723	2,05,844	1,68,233	3,74,077
FY 20-21	15,815	179	15,994	5,82,484	1,81,606	7,64,090
FY 21-22	9,882[1]	265	10,147	27,99,760	1,86,153	29,85,913

Table 22: Year-wise categories and catalogues on GeM

1. Approx. 5500 categories sanitized to prevent misuse by unscrupulous Buyers or Sellers; approx. 433 new categories added in FY21-22

There is further high degree of growth expected for GeM given increasing adoption trends across central as well as state Buyers and new functionalities envisaged for the new GeM platform. Basis the historical growth trends and assessment of current ongoing initiatives, below year-wise growth potential trajectory is envisaged for GeM:

Financial Year	Total Actual GMV (INR Cr.) *(excluding GST)*	No. of Transactions or orders	No. of transactions with order value <= 5 Lakhs	No. of transactions with order value > 5 Lakhs	No. of Buyers transacted	No. of Sellers transacted
FY 23-24	2,40,000 – 3,00,000	42,00,000 – 60,00,000	40,00,000 – 57,00,000	2,00,000 – 3,00,000	132,000 – 142,000	1,65,000 – 1,75,000
FY 24-25	3,00,000 – 4,30,000	50,00,000 – 70,00,000	48,00,000 – 66,00,000	2,50,000 – 4,00,000	165,000 – 180,000	2,10,000 – 2,30,000
FY 25-26	3,90,000 – 5,60,000	58,00,000 – 80,00,000	55,00,000 – 76,00,000	3,00,000 – 4,50,000	205,000 – 245,000	3,50,000 – 4,00,000
FY 26-27	4,60,000 – 6,70,000	70,00,000 – 88,00,000	66,00,000 – 83,00,000	3,50,000 – 4,80,000	245,000 – 320,000	4,20,000 – 5,00,000
FY 27-28	5,60,000 – 8,00,000	78,00,000 – 100,00,000	74,00,000 – 94,00,000	4,50,000 – 5,50,000	290,000 – 410,000	5,00,000 – 6,20,000
FY 28-29	6,70,000 – 9,60,000	90,00,000 – 115,00,000	85,00,000 – 109,00,000	5,00,000 – 6,00,000	340,000 – 510,000	7,00,000 – 9,50,000

Table 23: Indicative growth projections for GeM

This is to be noted that the above projections are indicative and should be considered for directional purposes only. These values should not be considered as a commitment from GeM.

The total duration of this Agreement will be a period of 6 (six) years from the date of signing of Agreement or 5 (five) years from the date of expiry of outgoing MSP's Agreement with GeM i.e., 1st Jan 2024, whichever is later. In addition, this Agreement may be extended for a maximum overall period of 3 (three) years, with 2 (two) year extension at one time and additional 1 (one) year extension the next time, on the same terms and conditions as contained in this RFP including all amendments, addendums etc. thereto. Any extension beyond 3 (three) years period shall be on mutually agreeable terms and conditions.

For this RFP, a hybrid (fixed + variable payout) financial model is proposed in order to primarily de-risk both stakeholders, GeM and MSP. Total payout is categorized into 3 components for this RFP (subject to LD if applicable) as defined below:

1.   **Fixed Platform Development fee:** Fixed payout of INR 15 (fifteen) Cr. per milestone basis successful completion of criteria under each milestone in Volume 1 Section 5 of this RFP. This payout shall be on one-time basis only for each milestone.

2. **Fixed O&M fee:** Yearly fixed fee of INR 40 (forty) Cr. for regular operations and maintenance of the platform. This shall be paid as INR 10 (ten) Cr. per quarter and will be applicable from the date of expiry for outgoing MSP contract i.e., 1st January 2024 onwards.

3. **Variable O&M fee:** This payout component will be linked to the overall performance of GeM platform, both existing or new, and will be applicable from the date of expiry for outgoing MSP contract i.e., 1st January 2024 onwards. This component will be payable per quarter and calculated as follows:

a. **Variable O&M fee** = 'Total No. of confirmed transactions" multiplied by the Variable fee factor as per applicable "Order Value" slabs as defined below. The total Variable O&M fee amount calculated henceforth will multiplied by Volume Factor as per applicable "No. of confirmed transactions" slabs defined below.

b. **Commercial Bidding Parameter (A):** There is only 1 bidding parameter for this RFP i.e., fee to be charged by the MSP per transaction for transactions with order value greater than INR 5 Lakh. This bidding parameter can be quoted up to INR 5000 as a maximum limit. The bidding parameter value shall include all taxes, levies, duties, etc. (excluding Goods and Services Tax).

c. **Variable fee factor:** This is defined as a fixed share of the Commercial bidding parameter for each applicable 'Order Value' slabs, as per below table:

Slab #	Order Value (excluding GST) per transaction *(in INR Lakhs)*	Variable fee factor *(% of A)*
Slab-1	0 < Order Value < = 5	2% of A
Slab-2	Order Value > 5	100% of A

Table 24: "Order Value" Slabs for Variable O&M fee

Slab #	No. of Confirmed Transactions in a financial year *(in Lakhs)*	Volume factor
Slab-1	0 < Total no. of transactions <= 50	100%
Slab-2	50 < Total no. of transactions <= 75	75%
Slab-3	75 < Total no. of transactions <= 100	50%
Slab-4	100 < Total no. of transactions <= 200	25%

| Slab-5 | Total no. of transactions > 200 | 10% |

Table 25: "No. of Confirmed Transactions" Slabs for Variable O&M fee

Basis the above definitions, below are select examples to further illustrate the calculation for the Fixed and Variable O&M fee payouts for a year:

Example (a):

No. of Transactions <= 5 Lakhs: 31,00,000

No. of Transactions > 5 Lakhs   : 2,00,000

Total no. of transactions   : 44,00,000

Bidding parameter (A)   : 3,000

Slab #	Order Value *(in INR Lakhs)*	No. of Transactions	MSP variable O&M fee *(INR Cr.)*
Slab-1	0 < Order Value < = 5	41,00,000	4100000*2%*100%* 3000 = 24.6 Cr.
Slab-2	Order Value > 5	3,00,000	300000*100%*100%*3000 = 90 Cr.
Total		44,00,000	114.6 Cr.

Table 26: Variable O&M fee calculation example (a)

Variable O&M fee accrued = INR 114.6 Cr.

Fixed O&M fee accrued = INR 40 Cr.

Total MSP payment: INR 40 Cr. + INR 114.6 Cr. = INR 154.6 Cr.

6.2 Payment guidelines for MSP

1. All the due payments to MSP up to the effective end of the Agreement, shall be made every quarter in a financial year (i.e., Apr-Jun, Jul-Sep, Oct-Dec, Jan-Mar) after making applicable deductions (if any) on account of Liquidated Damages, etc. as defined in this RFP. In a Financial Year, for calculation of the variable O&M fee every quarter, the volume factor to be applied on the 'Total no. of confirmed transactions' in that quarter will also take into consideration the 'Total no. of confirmed transactions' in the preceding quarters, as explained in below example (bid parameter assumed to be INR 3000).

| Quarter | Total No. of confirmed transactions (Lakhs) | | | | Variable O&M fee calculation | Quarterly variable O&M fee |
	Order Value <= 5 Lakhs	Order Value > 5 Lakhs	Total	Cumulative Total (Slab)		
Q1	19	1	20	20 (Slab 1)	19L*2%*3000 + 1L*100%*3000)*100%	41.4 Cr.
Q2	19	1	20	40 (Slab 1)	19L*2%*3000 + 1L*100%*3000)*100%	41.4 Cr.
Q3	28.5	1.5	30	70 (Slab 2)	Slab 1: 10L transactions [(50L-40L)*(28.5/30)* 2%*3000) + (50L-40L) *(1.5/30))*100% *3000)] *100%	20.7 Cr. + 31.1 Cr. = 51.8 Cr.
					Slab 2: 20L transactions [(20L*(28.5/30)*2%*3000) + (20L*(1.5/30)*100%*3000)]* 75%	
Q4	42.5	2.5	45	115 (Slab 4)	Slab 2: 5L Transactions [(5L*(42.5/45)*2%*3000) + (5L*(2.5/45)*100%*3000)]*75%	8.4 Cr. + 27.9 Cr. + 8.4 Cr. =
					Slab 3: 25L transactions	

					[(25L*(42.5/45)*2%*3000) + (25L*(2.5/45)*100%*3000)]* 50%	44.7 Cr.
					Slab 4: 15L transactions [(15L*(42.5/45)*2%*3000) + (15L*(2.5/45)*100%*3000)]* 25%	

Table 27: Quarterly variable O&M fee calculation illustration

2. In a quarter, 'Total no. of confirmed transactions' and corresponding 'Total no. of confirmed transactions' slabs for each order, once determined at the end of the quarter, shall remain constant, irrespective of any cancellations / rejections / refunds, for the 'Total no. of confirmed transactions' slab calculations and MSP fee computations in subsequent quarters.

3. Variable O&M fee for each order will be 100% payable in the quarter of successful contract/ order placement for both products and services on GeM platform.

4. Confirmed transactions refer to successful order/ contract placement on GeM platform.

5. Initial order value (excluding GST) will be taken into account for classification of transactions into Order Value slabs. Any subsequent change in order value arising out of quantity variation, tax variation, price variation or partial cancellations will not be taken into account for variable O&M fee calculations. Any child contract issued out of parent contract terms & conditions, e.g., option close, etc. shall not be counted separately as a transaction.

6. For any cancellation post successful order placement, only 10% of the due variable O&M fee as defined above shall be payable to MSP. MSP should adjust the fee payable corresponding to such orders in next quarter invoicing cycle, as applicable.

7. **Overall Quarterly Payout to MSP = Fixed Platform Development fee (if applicable basis milestones defined in Volume 1 Section 5 of this RFP) + Fixed O&M fee + Variable O&M fee basis confirmed transactions on the GeM portal in the quarter + Change request payout (if any) – Applicable Liquidated Damages and Deductions for the quarter (if any) – Recoveries for payment done by GeM on behalf of MSP (if any)**

8. Purchaser shall make payments only to the MSP at the time and in the manner set out in this section of the RFP subject always to the fulfilment by MSP and Consortium Partners of their obligations herein, except for the payment required to be made to the internet service provider providing internet bandwidth and connectivity. The payment to the internet service provider shall be made in accordance with clause 2.3 in Volume 3 Section 2 of the RFP. The payment made by the Purchaser to the internet service provider shall be set off by the Purchaser from the payments to be made to the MSP.

9. The MSP shall raise a quarterly invoice for the payment payable to MSP within the first week of the subsequent quarter via an automated SLA and payment management tool. The invoice shall include a breakup of no. of orders/ transactions, individual value of the orders / contracts, separately for products and services, with base price and taxes captured separately, along with the payment due per order / contract in the quarter. The invoices shall also include last quarter's payment release statement and payments released so far in that year.

10. MSP shall provision for an automated SLA and payment management tool for efficient invoice management and processing between GeM and MSP including functionality to upload invoices and supporting documents, review and process invoices

11. The MSP shall also submit all the agreed system-generated reports and supporting documents at the end of each quarter with clear calculations such as MSP fee breakup, SLA monitoring reports, Attendance records, Resource Deployment Plan, Liquidated Damages, Deductions, etc. as agreed jointly between GeM and the bidder through the automated SLA and payment management tool

12. The MSP shall be paid as per the FY quarters, any adjustment based on the onboarding time of the MSP, if needed, will be done on a pro-rata basis

13. GeM will examine the invoices and SLA reports raised by the MSP and will reconcile the payments every quarter. The due payments will be released to MSP after reconciliation, deduction of applicable LDs (if any) as per the SLAs defined in Volume 1 Section 8.6 of this RFP and any other deductions as per this RFP. GeM shall endeavour to release the Payment within 45 days of MSP raising the invoice.

14. Change request payout will be defined as a function of change pricing defined as per the Change Control mechanism in Volume 1 Section 8.7 of this RFP.

15. In the period between the date of expiry for outgoing MSP contract i.e., 1st January 2024 and Go-Live of new platform, both Fixed and Variable O&M fee shall be paid using the tools available in the current GeM platform, if needed

7. Compliance

1. For a platform like GeM, it is imperative that the highest standards applicable are adhered to. In this context, the MSP will ensure that all solution components in this project are certified and follow the applicable standards. The following table depicts the minimum number of standards on which GeM intends to get certified on along with the timelines:

Area	Standard/ Certification	Timelines
Security	CERT-IN and ISO 27001	Within 6 months of Go-Live
BCP	ISO 22301 and ITSM	Within 6 months of Go-Live
IT Governance	COBIT	Within 6 months of Go-Live
IT Operations	ISO 20000 and ITIL	Within 6 months of Go-Live
Testing & Quality	STQC (as mentioned below)	Within 3 months of Go-Live
Document Management	ISO 19475	Within 6 months of Go-Live

Table 28: Certifications

Component	Testing & Audit to be conducted
Enterprise Procurement System hosted at www.gem.gov.in	1. Functional Testing 2. Performance Testing 3. Web Application Security Testing
Hosting Infrastructure	1. System Architecture Review & Deployment Architecture 2. Process Audit (CVC, IT requirements) 3. Vulnerability Assessment 4. Penetration Testing
Data	1. Audit of Data Security in Storage 2. Audit of Data Security in Communication
Security Processes	1. ISO 27001 Process Audit
Service Levels	1. SLA Audit
Evaluation and Statement of	1. Compliance Verification – GFR 2017 2. Compliance Verification – CVC Guidelines

Conformity to Standards & Guidelines	3. Compliance Verification – IT Act 2000 and its Amendment 2008 4. Compliance Verification – Guidelines for compliance to Quality requirements of eProcrement Systems 5. Compliance Verification - MeitY EPS Guidelines (Other Requirements) 6. Analysis of review, testing and audit reports of EPS

Table 29: STQC Audit Requirements

2. The Standard/Certification will be the latest version at the time of implementation. In case any standard/certification is withdrawn or replaced with a new standard/certification, the MSP has to ensure that the new standard/certification is taken within defined timelines or within 6 months of the declaration of such change. The cost required for such certifications will be borne by GeM. The Cost relating to compliance with the above standards / certifications including documentation etc. will be the responsibility of the MSP.

3. Apart from the above, the MSP need to ensure compliance of the project with

   a. Government of India IT security guidelines and other guidelines/ notifications applicable to intermediaries/ e-commerce platforms including provisions of:

      i. The Information Technology Act, 2000" and rules framed thereunder and amendments thereof

      ii. Guidelines and advisories for information security by MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

      iii. Guidelines published by UIDAI issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

      iv. E-SAFE Guidelines for Information Security by MeitY (Government of India) issued till date of publishing of tender notice. till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

      v. E-Governance Standards for Preservation Information Documentation of e-Records by MeitY (Government of India) till the date of publishing of tender

notice. Periodic changes in these guidelines during project duration need to be complied with.

      vi.   E-Governance Standards on Biometric Standards (if applicable) by MeitY (Government of India) till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

    b.   Central Vigilance Commission (CVC) guidelines till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

    c.   Framework and Guidelines for Use of Social Media for Government Organizations by MeitY (Government of India) till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

    d.   Guidelines for Indian Government Websites by MeitY (Government of India) till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

4. GeM or its nominated agency have the right to conduct audits to ensure compliance of GeM setup to all relevant standards/ certifications. In such cases, MSP shall provide GeM or its nominated agency access to or a copy of any information, document, data, etc. promptly on a request made by GeM or its nominated agency.

5. In case of any additional standards / certifications apart from the above list, compliance timelines will be decided based on mutual agreement between GeM and MSP.

6. In case MSP fails to obtain the above certifications / standards, for reasons solely attributable to the MSP, within the timelines as mentioned in this RFP, Liquidated Damages of 0.2% of Annual Fixed O&M fee (over and above the 20% cap on Liquidated Damages as mentioned in Volume 1 Section 8.6 of this RFP) shall be levied on the MSP for each day of delay over and above mentioned timelines.

8. Annexures

8.1 Annexure A - Business Architecture & Processes

8.1.1 Business Architecture

This section describes the indicative business architecture for GeM, as per the business objectives and understanding of the process bottlenecks in the current procurement process. The overview of the architectural components (indicative) is shown in the figure below. The MSP shall automate the processes detailed in this section to the extent possible.

While all the current processes and workflows have been indicatively captured in the Business Architecture section of this RFP, it should be noted that there may be certain changes in these processes and workflows as a result of ongoing development of features & functionalities in the period between release of this RFP and MSP onboarding or as an outcome of ministerial guidelines impacting the scope of GeM (e.g., onboarding of cooperatives, etc.). Hence final business implementation should be as per the requirements finalized and documentation (BRD, FRS, SRS, HLD, LLD, system architecture, etc.) approved during the design phase as mentioned in Implementation Schedule in this RFP.
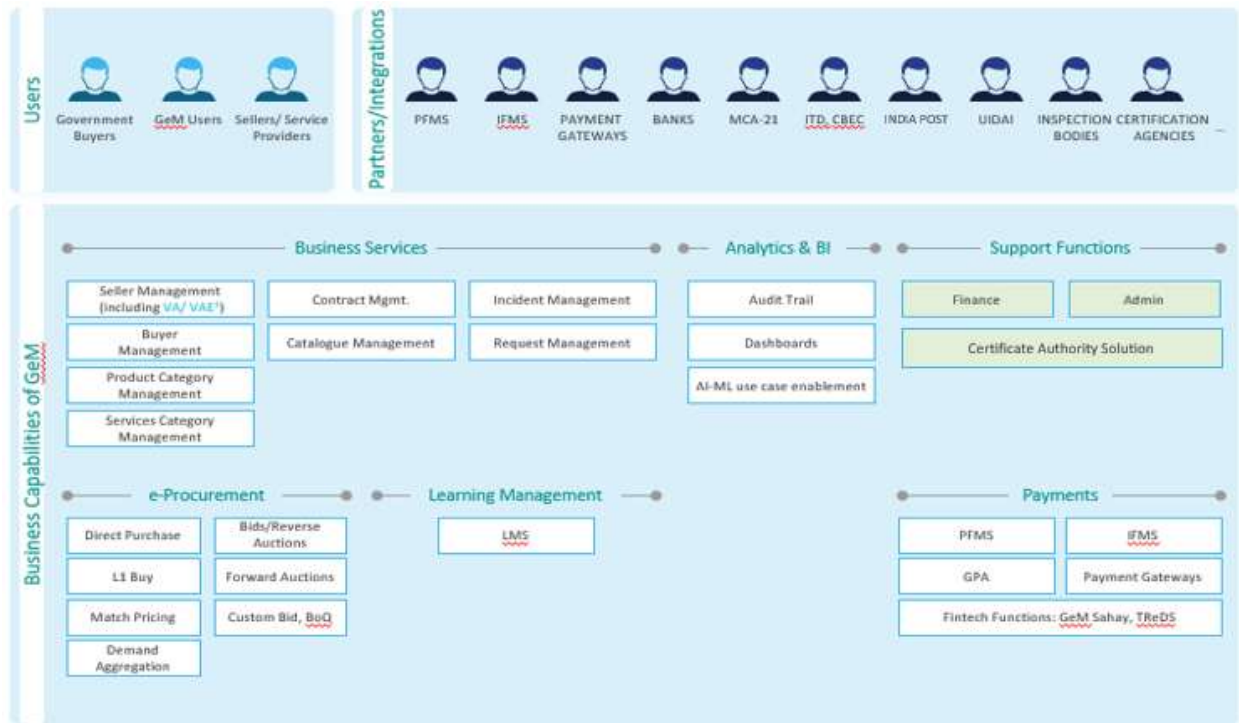
Figure 5: Business Reference Model

Users:

The key users for GeM are from Government Buyer departments, the GeM team, Sellers/ Service Providers, and GoI. User account creation is a self-service facility with an approval workflow approved by a competent authority. The application will be accessible to the following user groups:

1. GeM internal users

    a. GeM Buyer Management Team

    b. GeM Seller/ Service Provider Management Team GeM Product Owner

    c. GeM Service Owner

    d. Contact Centre

2. Government Buyers

    a. HoD/ Primary Buyer

    b. Procurement Officer

    c. Consignee

    d. DDO/ PAO

    e. Technical Evaluator

    f. Indenter

    g. Other user roles created in the future (Competent Authority, Verifying Authority, junior procurement personnel, legal and finance officers, etc.)

3. Sellers/ Service Providers

4. Partners

5. Third Party Agencies

Partners:

The key partners for the system would be various organizations such PFMS, IFMS, Banks (including bank wallets), Payment Gateways, NIC, Ministry of Corporate Affairs, Tax agencies like Income Tax Department, GSTN, CBIC and State Tax Departments, UIDAI for Aadhaar services, MCA-21 for Company verification purposes, etc. The seamless integration with these partner systems would enable automated validation and verification of suppliers or Buyers who want to be a part of the GeM system, payments, and smooth, reliable and real time functioning of the other business processes on GeM.

Third Party Agencies: Third party agencies envisioned to be integrated with GeM are inspection agencies, credit rating agencies, logistics players, Chartered Accountants, and others as per requirement. They will be responsible for different work streams, which may be outsourced to them, e.g., credit rating agencies for providing financial health of supplier, inspection agencies for conducting inspection of products & Services and Chartered Accountants for authentication of supplier registration & tendering related documents.

Channels:

The information dissemination on the GeM system will be done through SMS, call, webchat and email. The GeM application will be available to its users through mobile client and web browsing channels.

Core business & technical capabilities:

As depicted in the business reference model, key business capabilities that need to be facilitated would be

1. Buyer & Seller Management Services which includes registration services for Buyer, Sellers and Service Providers

2. Product & Services Management, which includes functionalities such as product/ service category management, specification management, etc.

3. Catalogue Management Services including content design & development of products & services catalogues

4. E-Procurement including functionalities such as creation and publication of bids, reverse auction, forward auction, custom bid, procurement through bill of quantity, direct purchase, L1 buy, demand aggregation, etc.

5. Contract Management Services, which includes e-Contracting, order processing and fulfilment, etc.

6. Analytics & BI, to help generate key reports and provide dashboards for internal and external stakeholders' reference. It will also be helpful in enabling features such as Seller/ Service Provider feedback & rating. Role based access to dashboards and reporting module through which stakeholders shall be able to generate and view relevant MIS reports

7. Learning Management System that will have informative audio and visual training and demo portal for hands-on training for all the stakeholders involved

8. A fully automated finance and payments module for both incoming and outgoing payments on GeM, supporting payments via PFMS, IFMS, GPA, payment gateways, etc.

9. Other support functions such as marketing and business development, administration, legal, etc.

10. Overall improvement and refinement of modules and sub-modules in alignment with GeM.

This includes implementation of additional interventions/ functionalities required within each modules/ sub-modules, as highlighted in, but not limited to, Volume 1 Section 8.1 of this RFP, in alignment with GeM.

8.1.2 Key Business Actors and Roles

8.1.2.1 Actors in the GeM system

Various Actors/Users that would be interacting with GeM would be:

1. **Government Buyers (Human):** The role of government Buyers (primary Buyer, consignee, DDO/ PAO, technical evaluator, Indentor, and other secondary Buyer users onboarded in the future) would be to initiate purchase process for goods or services, receive goods, and approve payments in the GeM marketplace, ensuring timely payments and quality inspections.

2. **Suppliers of goods and services (Human):** These would be the Sellers/ Service Providers in the GeM system. The Seller shall hold the responsibility to ensure the accuracy and integrity of all information shared, the quality of products and services sold and the timeliness of the delivery.

3. **Seller Management Team:** The role of Seller Management Team is to formulate the eligibility criteria for the Sellers/ Service Providers and lead the entire supply chain management. It would be accountable for maintaining eligibility rules & criteria of vendors in the system against which Sellers/ Service Providers can be verified.

4. **Product & Services Category and Catalogue Management Team:** The role of Product and Services Management Team is to manage product and services categories and catalogues end to end including category creation, approval, brand and OEM creation, product approval inspection related activities, maintaining marketplace sanity, etc.

5. **External systems:** Integrations with external systems will help support key processes (indicative list of external integrations provided in External Integrations section in Volume 1 Section 8.1 of this RFP). For instance,

   a. **UIDAI (External IT System):** These would provide authentication of the identity of Buyer, Seller/ Service Provider, etc.

   b. **Banks (External IT System):** These integrations would facilitate payments (both incoming and outgoing)

c. **Tax Agencies like ITD, etc. (External IT System):** These would provide detailed tax verification information for the vendor during registration or during the bidding process. These would be essentially automated actors and not require human intervention.

6. **GeM IT and Admin Departments:** These users would provide the non-functional/ infrastructure support to GeM via various administration tasks such as application, middleware, database, network, storage, server, identity, SOA, and BPM, user role & privileges creation, etc.

7. **Incident Management Team:** This team would handle the incidents raised against either Buyers or Sellers/ Service Providers on account of deviations from GeM policy. The incidents will be governed by GeM's Incident Management Policy

8. **Customer Service Management Team:** This team would oversee the customer service operations and ensure proper compliance

8.1.2.2   Roles in the system

The various actors who would interact with the GeM system would work with the following indicative business roles:

1. **Vendor Manager:** Approval authority for Seller/ Service Provider creation

2. **Contract Manager:** Responsible for contract management

3. **Product/service Owners:** Approval authorities for product & service addition/modifications/product specification creation and maintenance

4. **Process Owner:** Process owners will be the approving authority for maintenance for maintenance of applications of products and services. They would not be using the application but would be the approval authority for any change requests related to the module they own

5. **Competent/ Verifying Authority:** Approval authority from Buyer organization

6. **Government Buyer:** Government Buyer from government procurement department, can be either primary or secondary user in the system. Secondary users currently include roles such as Consignee, DDO/ PAO, Technical Evaluator, and Indentor

7. **Primary Buyer User:** These would be responsible for approval of creation of secondary

users within a particular government department like consignee, finance approvers, etc.

8. **Consignee:** Government consignee from government procurement department to receive consignments (secondary user)

9. **Sellers/ Service providers:** All vendors/ suppliers/ Sellers/ Service Providers, including OEMs, OSPs and resellers, in the GeM system

10. **Bidder:** Any Seller/ Service Provider participating in the bidding process through the portal

11. **Auctioneer/ FA Seller:** Any government department auctioning off products as part of a forward auction

12. **Buyer - internal users:** Not owners of the particular bid but other department users that help in evaluation, answering pre-bid queries, issuing clarifications, admin tasks, etc. – e.g., technical evaluator, etc.

13. **IT Admins:** Will provide IT support such as Identity management, database, middleware, Network, Email Messaging, Analytics & BI Admins, Server Admins, Security Admins etc.

14. Inspection approvers/ **Inspectors**

15. Auditors and vigilance officers

16. **Bid Officer:** Responsible for online bid management

17. **Verification Service provider:** External verification agencies/ CAs used to verify Seller/ Service Provider documents

18. **Helpdesk Support:** Contact centre executives

8.1.3   Registration

The GeM system provides the registration process for Buyers and Sellers/ Service Providers.

8.1.3.1   Buyer Registration

In Government Buyer Registration, there would be two types of users – HOD or Primary Users and they will create Secondary Users, i.e., business users with one or more of the following roles – Indentor, Technical Evaluator, Buyer, Consignee, Paying Authority/ DDO.

8.1.3.1.1   e-Registration of Primary User of a Government Buyer:

As can be seen in the figure below, the registration of Buyer would begin with addition of a department/ organization HOD or primary user to the GeM:
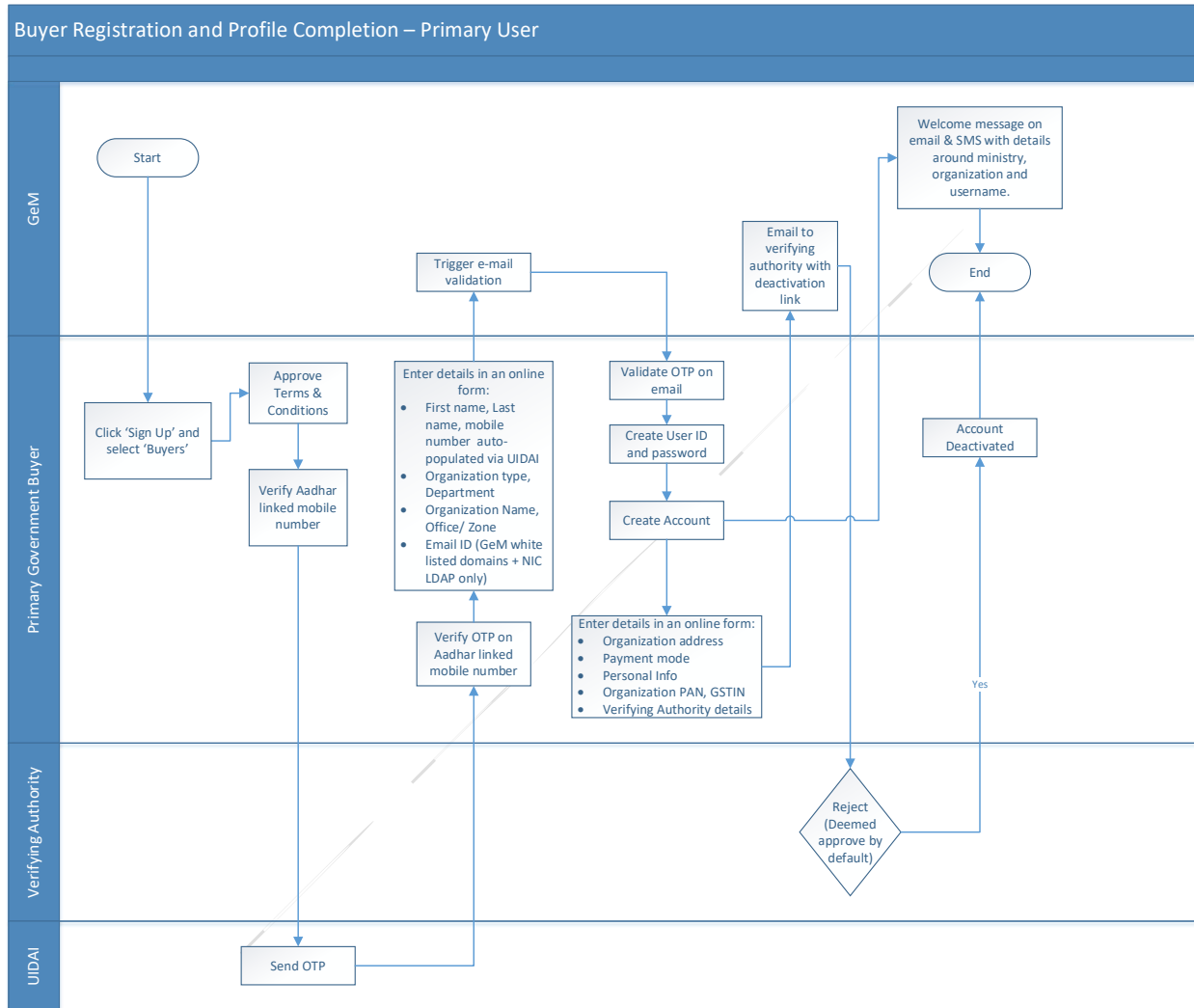
Figure 6: Buyer Primary User registration process flow

Process details and related system functionalities			
#	Process Steps	#	System Functionality
1	For new user registration, the Buyer will have to input Aadhaar and the Aadhaar linked mobile number and verify the details via OTP received on his/ her mobile	1.1	Integration with UIDAI
		1.2	Automatically capture name from Aadhaar database
2	First name, last name, mobile number of the user gets get auto-populated from Aadhar database. The Buyer needs to add all required details in the online registration form and attach all required documents. For example: 1. Organization Type, Department 2. Organization name, Zone 3. Email ID (GeM white listed domains + NIC LDAP) 4. User ID Then, validate the OTP sent to the email ID	2.1	Validate email ID is LDAP enabled
		2.2	Trigger OTP for verification to email ID & verify using Buyer input
		2.3	Organization hierarchy master database and user mapping
3	Buyer creates User ID and account. Post account creation the GeM system will send a welcome email/SMS with details such as Ministry name, department name, office name and User ID	3.1	Automated email and SMS post Buyer registration
4	Buyer will login to GeM and enter additional details and complete the profile such as: 1. Organization address 2. Preferred payment mode 3. Personal Info (Name, Designation date of retirement, etc. - to be fetched from NIC LDAP else user inputted) 4. Organization PAN, GSTIN 5. Details of verifying authority	4.1	System verifies the level of verifying authority (same/above) by checking if VA email ID is NIC LDAP enabled and triggers validation email with deactivate profile option Only whitelisted domains or NIC LDAP email IDs are allowed for VA
5	Email sent to Verifying Authority to validate the primary user. In case verifying authority	5.1	Automated email and SMS post Buyer registration

Process details and related system functionalities			
#	**Process Steps**	**#**	**System Functionality**
	rejects the primary user profile, the account is deactivated.	5.2	Functionality to transfer the role of primary Buyer to another individual post authentication, and create and manage divisions & secondary users

Table 30: Buyer primary user registration process & functionalities

8.1.3.1.2 e-Registration of a secondary User to an existing Government Buyer:

This process is the second step of the government Buyer registration process. In this process, registered primary user initiates the process of secondary user registration for appropriate roles such as that of procurement officer, consignee, indenter, etc. Secondary users get an invitation link after user addition/activation by primary user. The primary user of the Buyer department also has the functionality to manage (update/ delete/ transfer) secondary user accounts.

As a prerequisite, all users should have an email ID either from GeM white listed domains or NIC LDAP. In case a user does not have a valid email ID as per above, primary user has to request for a @gemBuyer.in email ID for that user via his GeM dashboard. Post getting @gemBuyer.in email. He may add secondary users as per below process.

Following is the detailed registration process for assuming the roles of procurement officer, consignee, indenter, etc. for the government Buyer department:
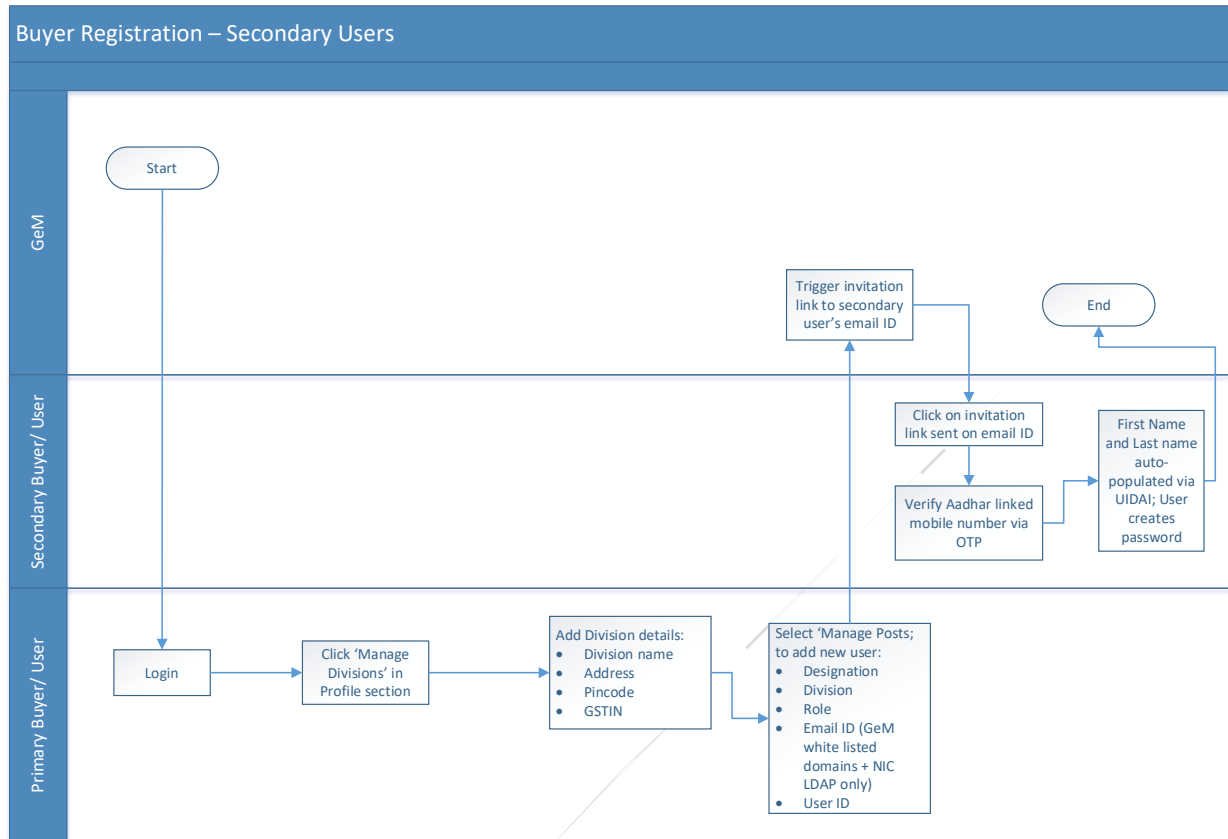
Figure 7: Buyer secondary users registration process flow

Process details and related system functionalities

#	Process Steps	#	System Functionality
1	For new user registration, the primary user will click on 'Manage Divisions' and add division details 1. Division name 2. Address 3. Pin code 4. GSTIN		
2	The primary Buyer will then add a new role	2.1	Automated invitation email sent to the

	by clicking 'Add new user' 1. Designation 2. Division 3. Role (Buyer, Consignee, DDO/ PAO, Technical Evaluation, Indentor) 4. Email ID (GeM White listed domains + NIC LDAP) 5. User ID		email ID entered to validate and verify account creation
3	The secondary Buyer will click on the link in the email to authenticate using Aadhar OTP. Post verification, their First name and Last name are auto-populated from UIDAI database. They will then create password to be used for future login.	3.1	Automated organization hierarchy mapping for all Buyer accounts (can be multiple roles per account and multiple secondary user accounts per primary account/ organization hierarchy)
		3.2	Auto-population of data via UIDAI database

Table 31: Buyer primary user registration process & functionalities

8.1.3.1.3   Additional interventions/ functionalities required:

1. Enable Buyer primary users to create custom secondary user accounts for stakeholders from other internal teams within the organization such as finance, legal, junior procurement personnel with flexibility to configure user-specific roles & privileges including adjustable financial limits (e.g., Buyer stakeholder specific procurement limits, category specific limits, access to customized dashboards basis their privileges, etc.)

2. Provision for workflows and shareable e-file where relevant stakeholders can add their remarks, approval, etc. to facilitate Buyer's internal processes, for example verifications, financial approvals, bid-related approvals, quality checks, etc., and route related documents to relevant Buyer users online on GeM

3. There should be complete automated process/workflow for user onboarding and user management while ensuring only valid/authentic government Buyer only may register

4. There should be provision for primary user to assign partial/complete workload of secondary user to another user. Functionality for primary Buyer user to transfer bid process, cart process, auction process, or any other procurement process from one individual to another in case the person overseeing the process goes on leave of absence, gets transferred

elsewhere,   etc.
(currently ongoing)

5. There should be roles and associated workflows and dashboards created for higher authorities (GeM Registration Authority, Verifying Authority) for managing (activation/deactivation, transfer), verification of primary user registration.

6. There should be a process to facilitate registration of verifying and competent authorities on GeM

7. There should be additional checks to prevent users to have access beyond retirement date.

8. There should proper checks to ensure that people of right designation/authority onboard the right roles.

9. There should proper checks to ensure that people of right designation/authority onboard the right roles under right organizations hierarchy

10. There should be provisions for a user to retrieve his/her lost account details

11. Develop, implement, and maintain a functionality or service for registration and management of B2B / B2C Buyers going ahead (after alignment with GeM)

12. Additional enhancements such as Buyer organization pin code to be captured and pre-filled fields wherever applicable, to be made to improve/ refine the process further

13. Functionality for deactivation of secondary user accounts basis system-driven logic, aligned with GeM (e.g., secondary users who haven't logged in to GeM in the last 2 years, provided no transaction should be pending against the user)

14. Allow authentication and integration with other Government user directories for authentication e.g., NIC SSO, etc.

15. Enable identity verification of users via banking channels for registration

16. Functionality for primary and secondary Buyer users to upload relevant documents. Type of documents to be submitted shall be configurable by GeM team via an Admin system functionality (e.g., official ID, DSC, etc.)

17. Integration with PAN and GSTIN for authentication and validation of data entered by Buyer users (if applicable)

8.1.3.2 Seller/ Service Provider Registration

All Sellers and Service Providers (new or rejoining on GeM) are required to go through the same registration process for onboarding on GeM, which primarily includes below three steps:

1. Creation of a primary user ID for Sellers/ Service Providers, preferably an authorized person such as Director of the organization or a Key Person/Proprietor/ ITR Signatory

2. Seller/ Service Provider profile completion and verification

3. Secondary user creation by the registered primary user of Sellers/ Service Providers, if required

Once a Seller account is closed, the Seller cannot create new account for one year from the date of account closure.

8.1.3.2.1 Primary user ID creation

The process flow for the primary user ID creation for the Sellers/Service Providers is depicted below:
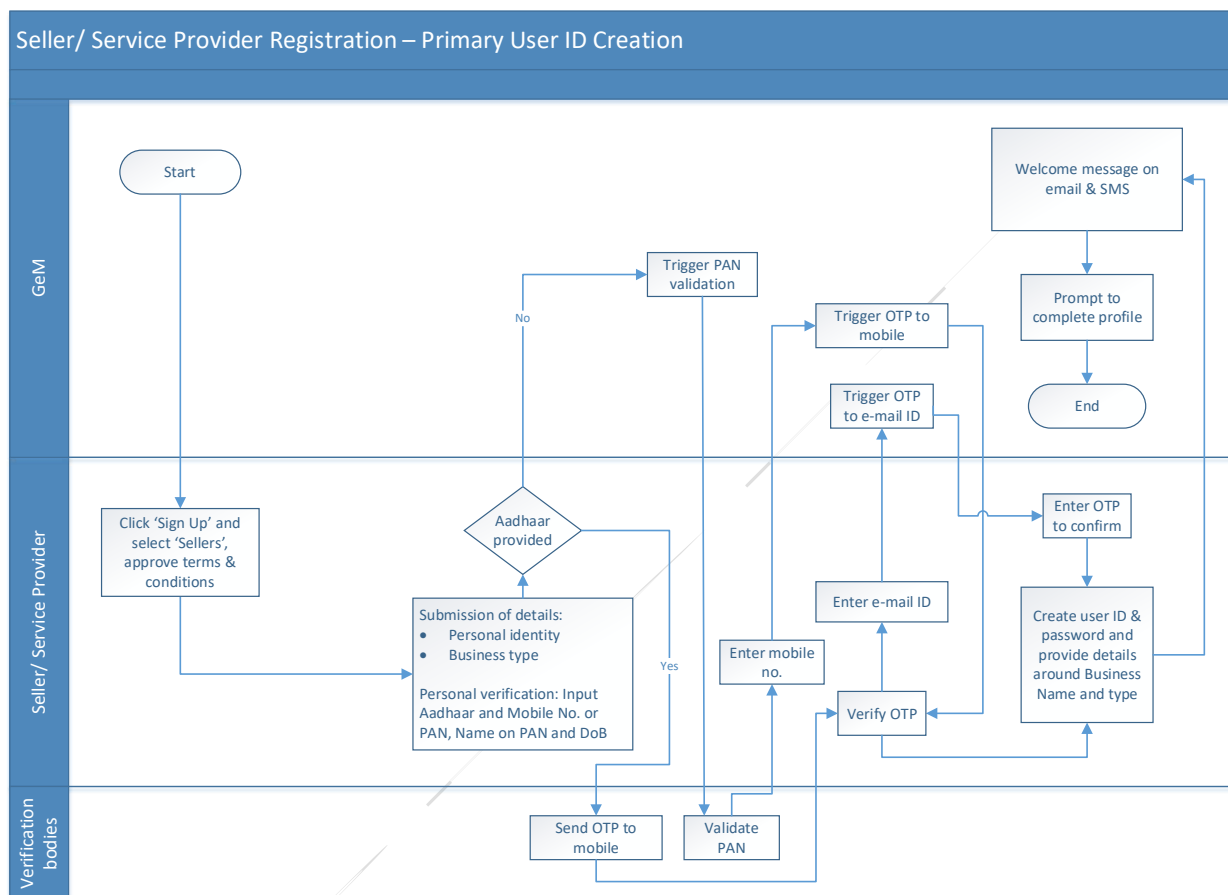
Figure 8: Seller/ Service Provider ID creation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	For new registration, Seller/ Service Provider will provide details about personal identity and business type and complete personal verification via	1.1	Store all details provided on cloud except Aadhaar linked personal information
		1.2	Integration with UIDAI and ITR services

				for real-time authentication
	1. Aadhaar and Mobile No. or 2. PAN and Date of Birth			
2	In case of PAN based registration, post PAN verification, Seller/ Service Provider will have to provide mobile no. and verify the same via OTP. However, once integration with Income Tax Department for mobile linked authentication of PAN No is completed, OTP based authentication with the linked mobile should be carried out.	2.1	Automated triggering of OTP for verification to mobile no. & verify using Seller/ Service Provider input	
		2.2	Integration with Income Tax Department for mobile linked authentication of PAN No. for real-time authentication.	
3	Post-verification, Seller/ Service Provider will have to provide e-mail ID and verify the same via OTP	3.1	Automated triggering of OTP for verification to Seller/ Service Provider's e-mail ID & verify using Seller/ Service Provider input	
4	Seller/ Service Provider should create user ID and password and provide details about business name and type	4.1	Store all details provided on cloud	
		4.2	Automated prompt for profile completion	
		4.3	Automated email and SMS post Seller/ Service Provider registration	

Table 32: Seller/ Service provider ID creation process & functionalities

8.1.3.2.2 Profile completion/verification or modification of Seller/ Service Provider

The Seller/ Service Provider will enter details such as Business PAN, CIN, bank account details, address details, etc. on GeM portal. GeM portal will trigger automated verification requests to various verifying authorities (ITR services, MCA-21, GSTIN, PFMS, Udyam, DIPP, etc.) integrated with GeM to verify the details provided by the Seller/ Service Provider.

Note: If verification from any of the partner organizations fails, GeM will by default consider the profile as incomplete profile. Seller will have to complete the profile before engaging in any other activities on the GeM portal.

The process flow for profile completion/verification or modification for the Sellers/Service Providers is depicted below:
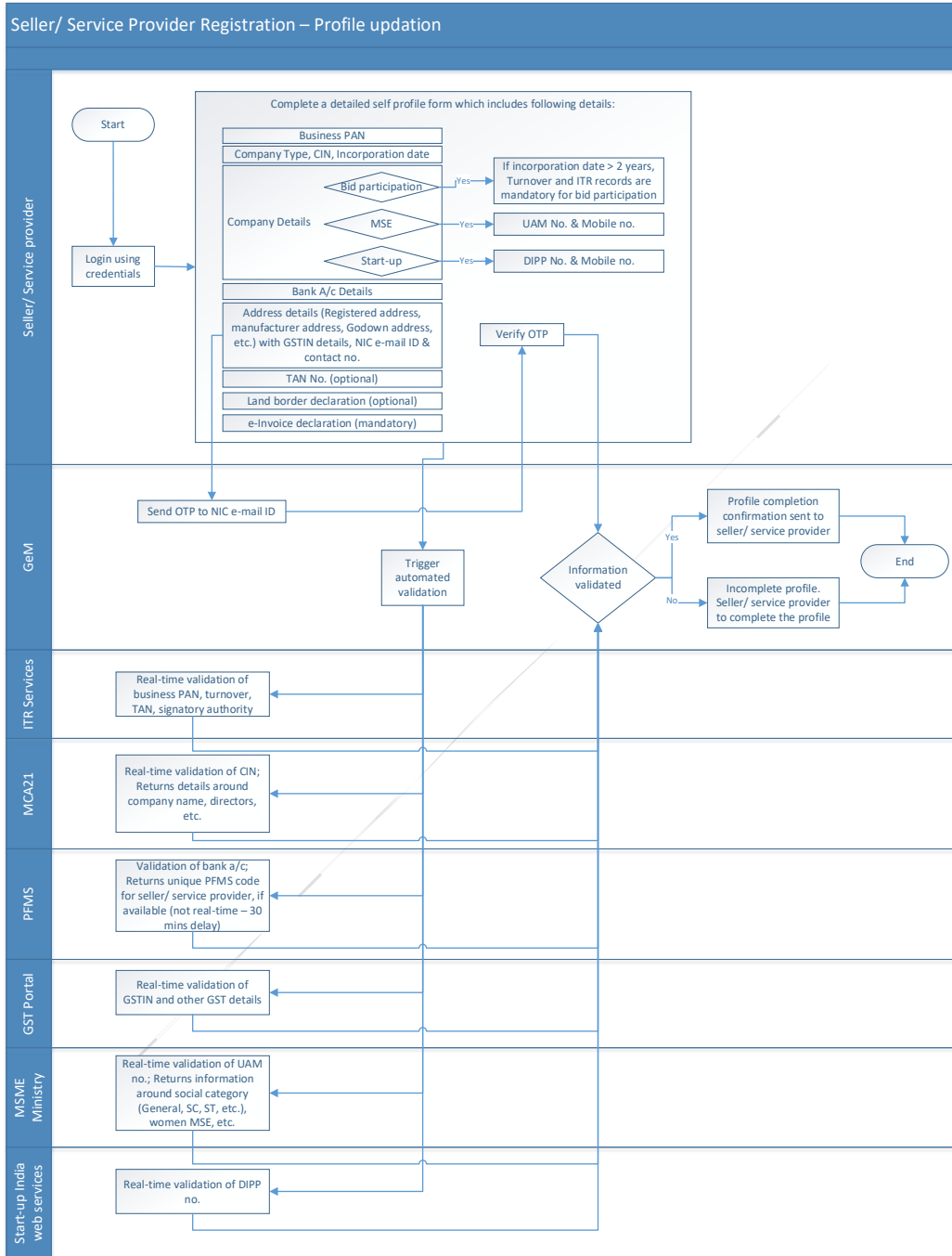
Figure 9: Seller/ Service Provider profile updation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Seller/ Service Provider enters required details in an online form and attaches all relevant documents, for example: 1. Business PAN 2. CIN 3. Incorporation date and other company details (bid participation, MSE, start-up, etc.) 4. Bank A/c details 5. Address details (Registered, manufacturer, warehouse, etc.) with GST details and NIC e-mail ID and contact no. 6. In case of MSE – UAM no. & mobile no. 7. In case of start-up – DIPP no. & mobile no. 8. TAN (optional) 9. Land border declaration (optional) 10. E-Invoice declaration (mandatory)	1.1	Automatically verify details provided by Seller/ Service Provider via integrations with ITR services, MCA-21, GST portal, PFMS, MSME Ministry, Start-up India web services, etc. in real-time/ near real-time
		1.2	Prompt Error Messages wherever applicable
		1.3	Update all details in the system and send confirmation e-mail to the Seller/ Service Provider

Table 33: Seller/ Service provider profile updation process & functionalities

Vendor Assessment: Vendor assessment is compulsorily conducted for OEMs who wish to apply for the OEM panel on GeM via a third party agency (currently done by QCI - a dashboard is available to QCI to view and manage Vendor Assessment requests). Vendor assessment can also be conducted for resellers. OEM panel offers Sellers/ Service Providers some additional privileges such as functionality to approve catalogues pertaining to their brands. Vendors with either a turnover of INR 500 Cr in any of the last 3 years, or vendors having Vendor Assessment (VA), or Vendor Assessment Exemption (VAE) are eligible to apply for the OEM panel.

1. **Vendor Assessment Exemption (VAE):** A vendor can apply for exemption from Vendor Assessment on GeM. Vendor is required to upload relevant documents (e.g., NSIC certificate, ministry related certificate for VAE, empanelment/ trusted vendor certificate), provide vendor details including address, contact details, etc. pertaining to the relevant category.,. The details are pushed from GeM to the third party agency via an API integration for

assessment of the documents and feedback on their validity.

2. **Vendor Assessment (VA):** Similar to VAE, a vendor can apply for a VA on GeM. Vendor is required to upload relevant documents (e.g., NSIC certificate, ministry related certificate for VAE, empanelment/ trusted vendor certificate), provide vendor details including address, contact details, etc. pertaining to the relevant category. The details are pushed from GeM to the third-party agency via an API integration for assessment of the documents and feedback on their validity as 'PASS/ FAIL' basis verification. In case of a PASS, third party agency also returns other details including production capacity, locations, etc.

Post VA approval or VAE attainment, the vendor is eligible to apply for the OEM panel.

8.1.3.2.3   Secondary user creation by registered Seller/ Service Provider

Primary users can create and manage accounts for secondary users by following the process detailed below:
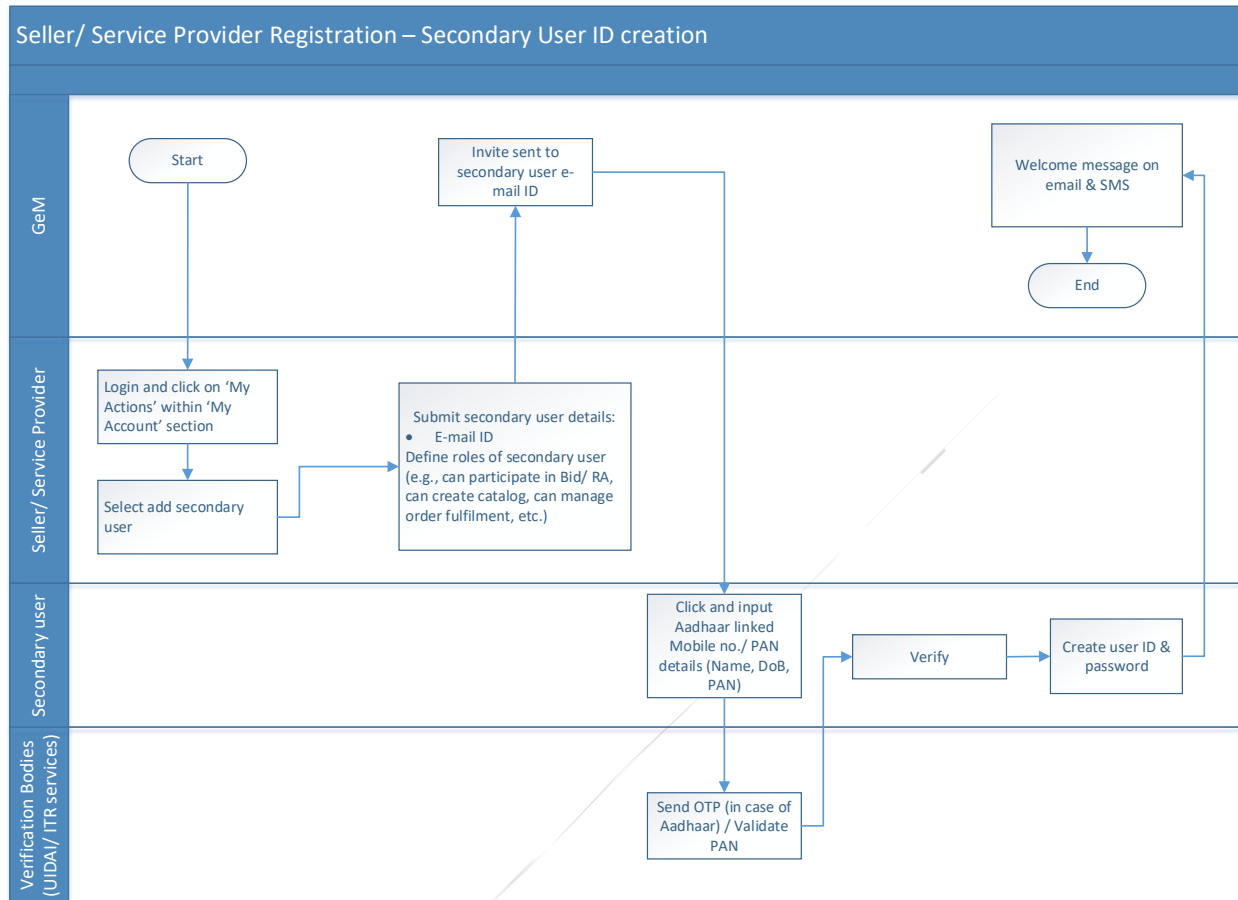
Figure 10: Seller/ Service provider secondary user registration

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	For new user registration, the primary Seller/Service Provider will click on 'My Actions' within 'My Account section' and add a new user by clicking 'Add secondary user'. The primary user will	1.1	Automated registration invite sent to secondary user's e-mail ID

	1. Provide secondary user's e-mail ID 2. Define roles of secondary user (e.g., can participate in Bid/ RA, can create catalog, can manage order fulfilment, etc.)		
2	The secondary Buyer will click on the link in the email to authenticate using Aadhaar/ PAN basis primary user account. They will then create a user ID and password for future login	2.1	Integration to UIDAI, ITR services
		2.2	Automatically capture name from Aadhaar database
		2.3	Secondary user and role mapping for all Seller/ Service Provider accounts
3	The GeM system will then send a welcome email/SMS to the user	3.1	Automated email and SMS post-secondary user registration

Table 34: Seller/ Service provider secondary user registration process and functionalities

8.1.3.2.4 Additional interventions/ functionalities required

1. Enable Seller Primary Users to create custom secondary user accounts for stakeholders from other internal teams within the organization such as product, finance, legal, etc. with flexibility to set user-specific roles & privileges (e.g., catalogue creation and upload, access to customized dashboards basis their privileges, etc.)

2. Allow Sellers/ Service Providers (mapped to a unique PAN) to create multiple divisions representing different business areas of the same Seller entity. For instance, ONGC to have different divisions for Petrochemicals and Power tagged to the same entity mapped with unique business PAN

3. Enable identity verification of users via banking channels for registration

4. Integration with FCRA online services (Foreign Contribution (Regulation) Act)/ FLLP (Foreign Limited Liability Partnership) for verification of data of foreign companies. More such integrations may be required in the future as GeM evolves

5. Briefcase facility to collect and save all relevant documents used on a recurring basis in bids etc., from Sellers/ Service Providers, e.g., MSE certificate, start-up certificate, turnover certification, relevant experience in case of a services related bid shall be made available *(currently ongoing)*

6. 'Holiday' option to allow Sellers/ Service Providers to mark non-working days and large

holiday periods should be implemented *(currently ongoing)*

7. There shall be requirement of mandatory registration for at least one director/ key person/ ITR signatory authority from each Seller/ Service Provider entity, with provision for the director/ key person/ signatory authority to nominate nodal officers to act on their behalf. Enforcement of key person validation with online/ offline functionality via verifying organizations such as QCI, etc.

8. Provision for automated back-end revalidation of external data at periodic intervals (e.g., CIN, UAM no., DIPP no., etc. etc.) *(currently ongoing)*

9. Configurable web-based push notifications for selected events (as configured by Sellers/ Service Providers) to ensure Sellers/ Service Providers are updated timely even when not logged into the platform

10. Functionality for Sellers/ Service Providers to upload relevant documents. Type of documents to be submitted shall be configurable by GeM team via an Admin system functionality (e.g., address proof for registered address of organization, incorporation certificate, etc.)

11. Enable registration via multiple types of PAN (e.g., local bodies judiciary PAN, etc.), and authentication using biometric, e-sign, PAN, etc.

8.1.4 Category Management

As a marketplace, one of the founding pillars of GeM is its products and services categories. Given the multitude of government Buyer organizations that transact on GeM and their large procurement needs, the scale, and the spread of type of transactions on the GeM platform is enormous. Currently, unique product and service categories are organized across four classification levels (L1 to L4) as per United Nations Standard Products and Services Code (UNSPSC) classification system. GeM will gradually transition towards Indian Trade Classification Harmonized System (ITC-HS) and consequently, modification or addition of further classification levels shall be needed. Category management process involves the following stakeholders:

1. **Category creator**: One who establishes new category section, classifies the category hierarchy, and assigns it to a relevant work group in the system

2. **Work group:**

    a. **Category maker:** One who defines the category configurations and specifications

b. **Category checker:** One who reviews and approves the category-related details

c. **Catalogue agent:** One who is responsible for reviewing and approving uploaded product catalogue and brands by the relevant Sellers within the category

Category creation and management process includes but is not limited to following:

8.1.4.1 Category Creation

Category creation involves design of Technical Parameters (TP) related to the products or services, assigning List of Values (LoV) corresponding to each TP and other category-related attributes such as ordinal parameters, dependencies between TPs, and TP based rule engines (e.g., higher is better or lower is better), etc.

There are four types of categories as highlighted by the category quadrant below:

1. Q1: Only OEM can participate in category

2. Q2: Only OEM & authorized resellers can participate in category

3. Q3: OEM & resellers can participate in category and OEM can manage resellers

4. Q4: OEM & resellers can participate in category, but OEM cannot manage resellers

The process flow for category creation is depicted below:
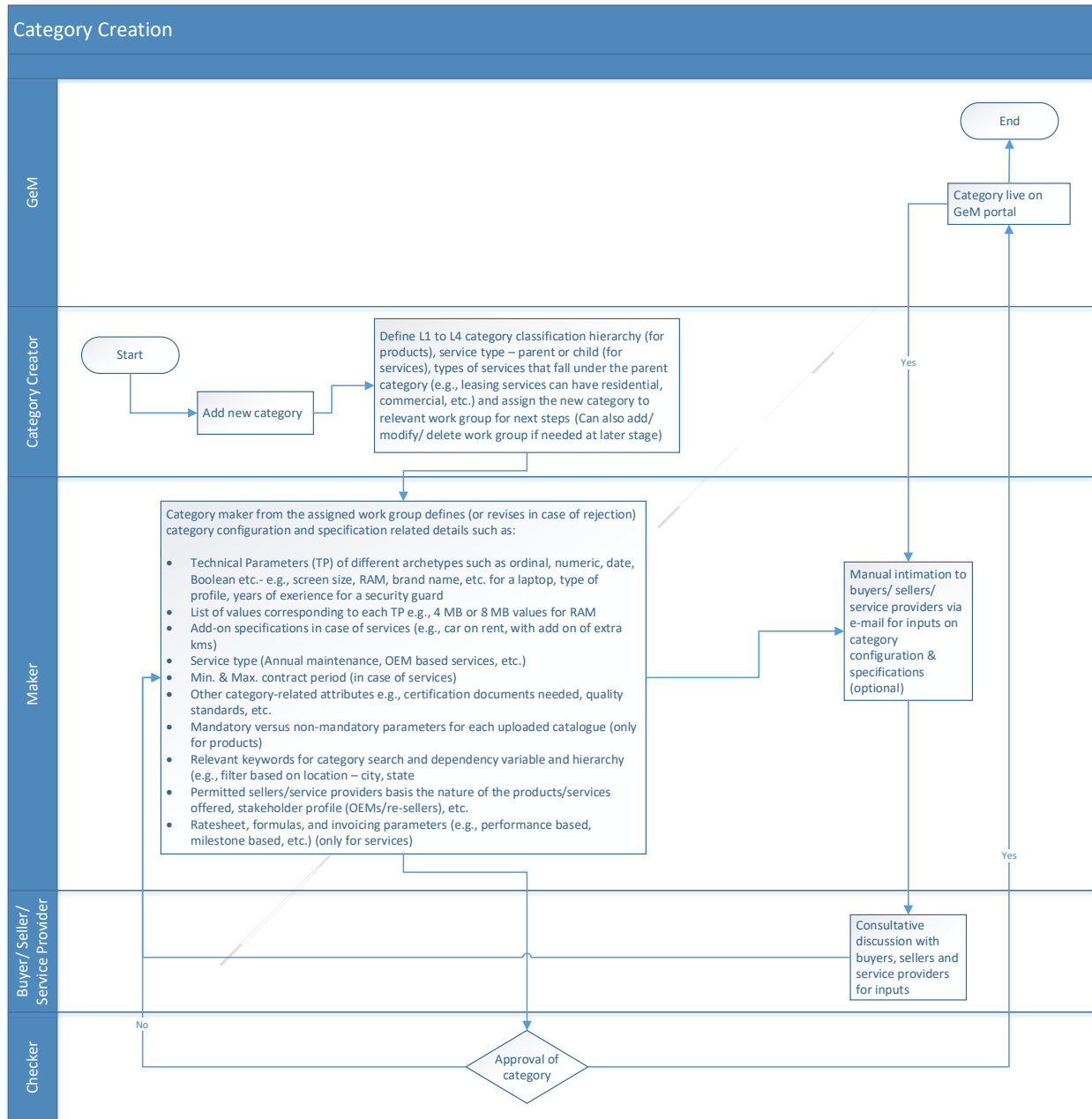
Figure 11: Category Creation

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1.	Category creator initiates establishment of a new category in the system, defines L1 to L4 category classification hierarchy, defines service type (parent/ child), types of services that fall under the parent category (e.g., leasing services can have residential, commercial, etc.) and assigns the new category to the relevant work group for next steps	1.1	Automated update of category hierarchy structure with each new category addition
		1.2	Feature to add/modify/delete work groups and specific individuals within a workgroup
2.	Category maker from the assigned work group defines category configuration and specification related details such as: 1. Technical Parameters (TP) of different archetypes such as ordinal, numeric, date, Boolean etc.- e.g., screen size, RAM, brand name, etc. for a laptop, type of profile, years of experience for a security guard 2. List of values corresponding to each TP e.g., 4 MB or 8 MB values for RAM 3. Add-on specifications in case of services (e.g., car on rent, with add on of extra kms) 4. Service type (Annual maintenance, OEM based services, etc.) 5. Min. & Max. contract period (in case of services) 6. Service category type (bid only service category (e.g., consulting), optional offer price service, etc.) 7. Other category-related attributes e.g., certification documents needed, quality standards, etc. 8. Mandatory versus non-mandatory	2.1	Category-wise details storage enablement
		2.2	Interaction with search module basis defined keywords in each category
		2.3	Interaction with other modules such as bid, L1 or Direct purchase for category specification and parameter-based buying on GeM

	parameters for each uploaded catalogue (only for products) 9. Relevant keywords for category search and dependency variable and hierarchy for filtering results (e.g., results filtered basis project location based on location – city, state) 10. Permitted Sellers/Service Providers basis the nature of the products/services offered, stakeholder profile (OEMs/re-Sellers), etc. 11. Rate sheet, formulas, and invoicing parameters (e.g., performance based, milestone based, etc.) (only for services) 12. TP based rules and weightages of LoV (For instance, in case a Buyer selects i3 processor as min. requirement for a laptop, then Sellers offering i5 and i7 are also allowed to participate. This is decided basis higher is better rule applied on weightages assigned to LoVs)		
3.	Submitted category by the category maker is reviewed, edited, sent back for changes/ or approved by category checker	3.1	Automated workflows for category creation, configuration, and approval
4.	Category is live on GeM portal once approved by the category checker		

Table 35: Category Creation process & functionalities

8.1.4.2 Category Maintenance:

Category maintenance involves regular revision of the TPs, list of values, and category-related features and functionalities in-line with changing demands of Buyers/Sellers, market growth and government policies. It allows category maker and checker to add or modify specifications in an

existing category as detailed below. Currently, only TPs and LoVs can be added to the category and not be modified or deleted. Only certain category-related attributes and, rules and configurations can be added, modified, or deleted (e.g., certification can only be deleted, configurations such as whether to allow products originating from certain countries, whether to enable pre-bid or no, and price bounds can be added, modified or deleted, etc.)

In case of services, currently TPs and LoVs can be added, deleted and the name can be modified. The required certifications can also be added, deleted or modified. However, Rate sheet can only be modified.
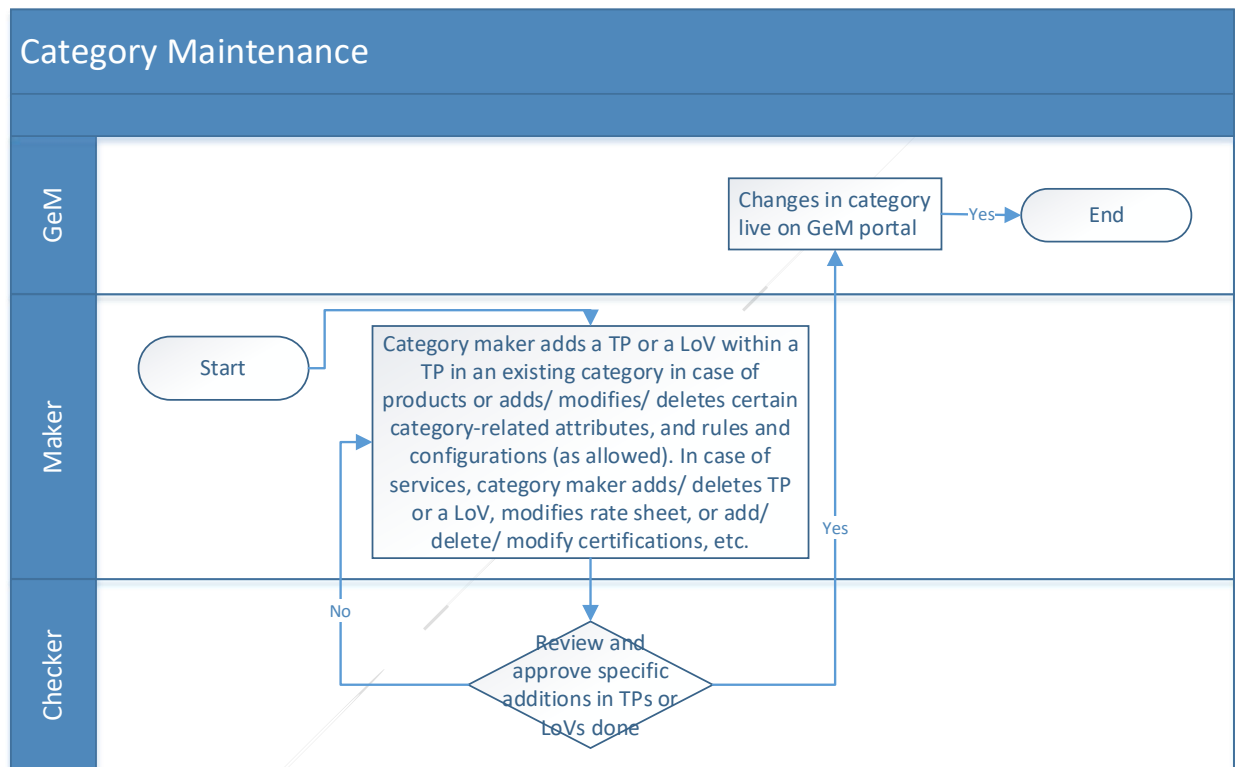
Figure 12: Category Maintenance

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**

1.	Category maker adds a TP or a LoV within a TP in an existing category in case of products or adds/ modifies/ deletes certain category-related attributes, and rules and configurations (as allowed). In case of services, category maker adds/ deletes TP or a LoV, modifies rate sheet, or add/delete/ modify certifications, etc.	1.1	Feature to add TPs and LoVs for products, add/ delete TPs and LoVs for services.
2.	Category checker reviews and reject/approve specific additions in TPs or LoVs done	2.1	Automated approval workflow with changes highlighted for checker
3.	Once approved, changes go live on GeM portal		

Table 36: Category Maintenance process & functionalities

8.1.4.3 Additional interventions/ functionalities required:

Category creation

1. During category creation, in case of multiple iterations between category maker and checker, iteration-wise changes / modifications should be highlighted or notified automatically for efficiency in category approval workflow

2. Assign a checker to sample test and verify product/ brand catalogues approved to be added in various categories

3. Automated notifications related to category (for Category Consultative Meetings and other information) to be sent to Buyers, OEMs, resellers, Service Providers, etc. on a configurable basis (currently ongoing)

4. The functionality of multiple invoicing options, and multiple units of measurements, quantity and formulae related to a service in the rate sheet should be provided (e.g., painting of a building vs. painting of a table may have separate unit of measurements, and calculation formulae)

5. Functionality to enable multiple units of measurements for product categories

6. There shall be a functionality to define mandatory versus non-mandatory parameters for each uploaded catalogue for services.

7. Enable macro-based, bulk upload of categories via upload of an Excel sheet containing details of multiple categories (including multiple invoicing options, multiple formulae, multiple units of procurement, and multiple rate sheets, etc. in case of services) in a pre-defined format

8. Hierarchical/ Nested dependencies should be expanded up to 8 levels from the current 4 levels

9. Additional options within service category type selection such as nomination based purchasing, percentage based tendering, etc.

10. Provision for category specific libraries – e.g., SLA library for services

11. Provision to add or modify classification levels (L1 to L4) upon transition from UNSPSC classification system to Indian Trade Classification Harmonized System (ITC-HS)

Category Maintenance

1. Allow category makers to add, modify as well as delete Technical Parameters, List of Variables as well as other category-related attributes, and rules and configurations (as aligned with GeM) for all categories live on GeM portal

2. Automated notifications to registered Sellers/ Service Providers highlighting the changes made to their respective categories should be issued.

3. Provision of a dashboard to view key metrics associated with a category (e.g., no. of bids linked to a particular category, Sellers/ Service Providers associated with the category, number of contracts signed, etc.

4. Relevance and accuracy of keyword search results should be optimized

5. Migration of category in any quadrant should be automated

8.1.5 Catalogue Management

E-Catalogues contain information about products and services available on GeM portal. Effective and strategic catalogue management ensures the quality of product data. Catalogue Management system supports the definition, storage, retrieval, and management of product/ service information throughout the e-procurement process.

8.1.5.1   Product Catalogue Management

Sellers (OEM, Resellers, etc.) have the functionality to broadcast their brands, products, and prices and introduce new brands/ products via the Catalogue Management System.

The lifecycle of a catalogue starts with creation of a brand for a category. Brand creation request can be clubbed with OEM panel request. OEM panel allows OEM to manage their re-Sellers, catalog, and authorizations. A catalogue is linked with the brand only. Brand can be registered, unregistered and unbranded. A catalogue is uniquely defined in GeM as a combination of brand and its golden parameters. A bid can be published on a catalogue, or the combination of specifications provided by Buyer.

In case of Q2 categories, reseller need to submit authorization code (generated by OEM via OEM panel and shared with reseller), category and brand within which they wish to upload a catalogue. Once the code is validated by the system, the authorized reseller is allowed to upload a catalogue within the specified category and brand.

Product Catalogue Management involves multiple sub-processes:

1. Catalogue creation

2. Catalogue approval

3. Catalogue modification

4. Brand/OEM request and approval

Each of these sub-processes have been explained in detail in the below section.

Sellers can view the catalogues they have published and the status of the ones they have created and submitted for approval via a dashboard. Depending on the catalogue status, the dashboard categorizes various catalogues into the following tabs:

1. Published: Catalogues live on GeM

2. Draft: Catalogues being created

3. Notified: Catalogues returned to Seller by approval team with suggestions to correct catalogue

4. Waiting for Admin Approval (Product Approval team)

5. Waiting for OEM Approval

6. MRP Change Request: Catalogues with pending MRP change requests initiated by Seller on account of MRP change or GST change. MRP change request can be initiated by the Seller by selecting the MRP change request option within 'Edit' option available for published catalogues. The Seller is required to submit relevant supporting documents that validate the MRP change and submit the same for approval. The approval team then vets the documentation provided and approves the request or notifies the Seller of their suggestions. In case of latter, Seller makes relevant changes and re-submits the request for approval. Once approved, the changes in MRP get reflected on GeM portal

7. Brand OEM Request: Pending Brand creation request raised by OEM

8. Expiry soon: A catalogue shows up in this tab 15 days prior to its expiry

9. Expired: A catalogue expires after 60 days of no activity after publishing.

10. Discontinued: List of catalogues discontinued either by Seller or by OEM

11. Rejected: List of rejected catalogues

Catalogue creation

A Seller can create and upload a new catalogue or pair with an existing one created by an OEM or another re-Seller.

A product catalogue can be created and uploaded by a Seller by providing the following information:

1. Product Specifications

    a. Golden parameters (directly contribute to price - e.g., in case of laptop - processor, RAM, etc.)

    b. Non-golden parameters (e.g., no. of USB ports, Bluetooth feature, etc.)

2. Characteristics (e.g., model no., brand, etc.)

3. Documents (e.g., certifications, MRP proof, catalogue brochure)

4. Product images: Three different images are mandatorily required to be uploaded

5. Prioritization: In case the catalogue is to be used in an upcoming bid, Seller can get the catalogue prioritized for approval by mentioning the bid ID

6. Product details (e.g., authorization from OEM, country of origin, Make In India (MII) – Yes/ No, Start-up – Yes/ No, Pricing & Slab discount, Stock details such as maximum stock available, minimum order quantity, locations, lead times, delivery locations serviced, etc.)

In case a Seller wishes to pair with an already existing catalogue, he/ she will have the functionality to edit the product details fields directly related to him/ her (e.g., stock details, locations, lead time, country of origin, etc.). Seller can also create clone specifications to create new catalogue with few changes in existing specifications.

The process flow for product catalogue creation is depicted below:
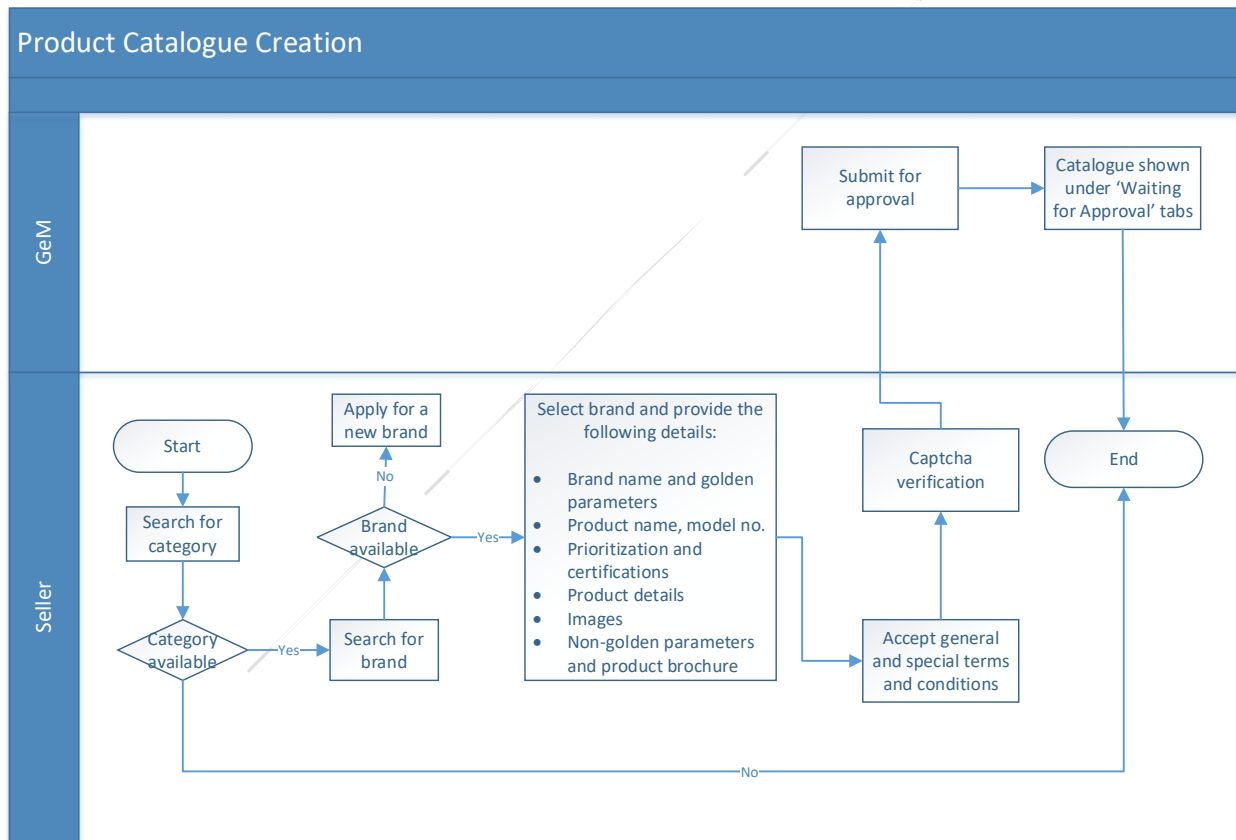
Figure 13: Products Catalogue Creation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Seller searches for category within which he/ she wants to upload a catalogue. In case a category is available, Seller searches for the brand.	1.1	Category and brand search
2	In case a brand is available, Seller proceeds to create the catalogue. If brand is not available, he/ she needs to apply for a new brand to be created		

3	After selecting the brand, Seller provides the following information in the order below:
	  1. Brand name and golden parameters
	  2. Product name, model no.
	  3. Prioritization and certifications
	  4. Product details
	  5. Images
	  6. Non-golden parameters and product brochure
		3.1	File upload functionality with system defined rules for file format and size

		3.2	Data and documents uploaded stored on cloud
		3.3	Integration with FSSAI and BIS certifications
		3.4	Defined algorithm to manage incoming queue for product approval from multiple Sellers. This algorithm adjusts priority on the basis of various parameters like a product for ongoing bid, a product for Covid-19 related categories, etc. The same algorithm is also defined for Brand/OEM panel
4	After providing these details, Seller accepts the general and special terms and conditions (category specific), completes captcha verification, and submits the catalogue for approval	4.1	Captcha code generation and validation
		4.2	Catalogue moves to the Waiting for Approval tabs

Table 37: Products Catalogue Creation process and functionalities

Catalogue Approval

Once the catalogue is created and submitted for approval, it goes to either the OEM, in case the brand OEM exists in the GeM system, or product approval team for review and approval.

Within GeM, as of now the catalogue agent from the product approval team is responsible for reviewing and approving product/ services catalogue and brands by the relevant Sellers within the category for upload. A Checker role who will review the MSP processed catalogue and related recommendations on sample basis, will be introduced in the process as highlighted in the additional functionalities section. The Checker may be from GeM.

The process flow for product catalogue approval is depicted below:
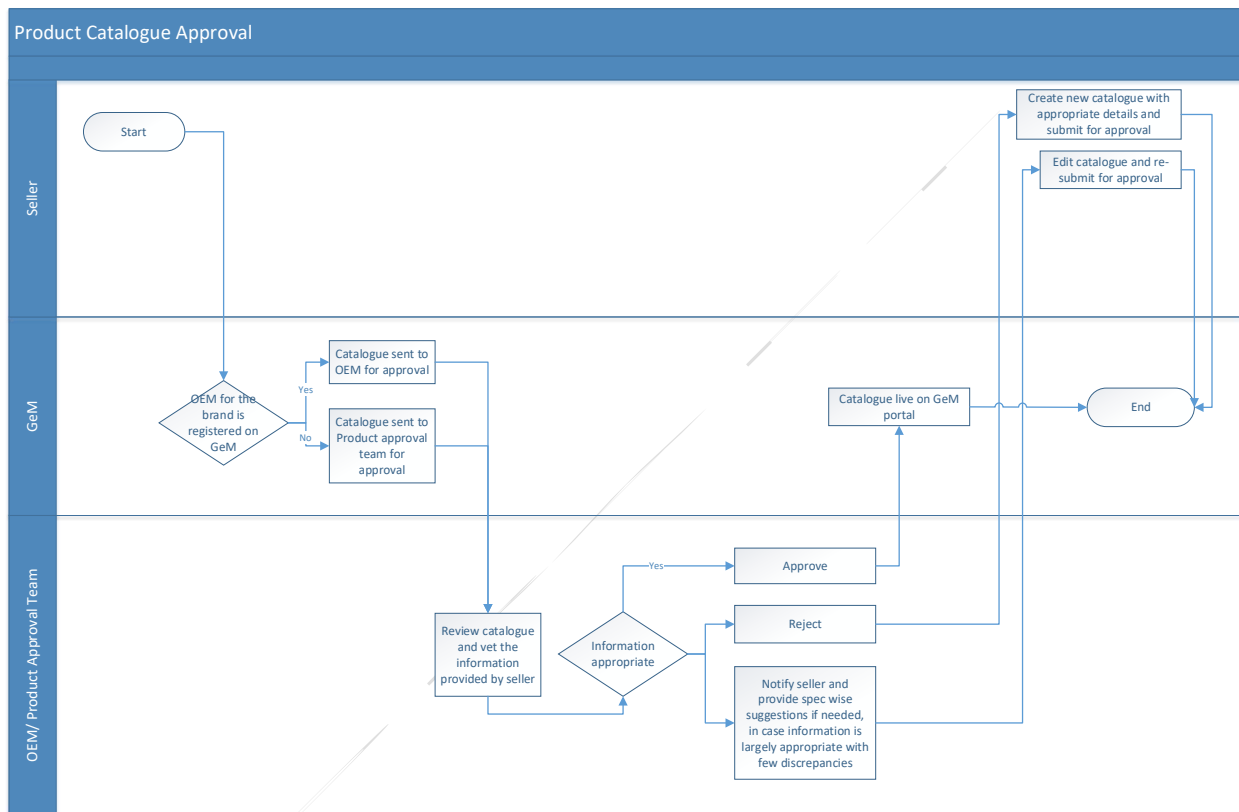
Figure 14: Products Catalogue Approval

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1		1.1	System checks for OEM and re-routes

	Post catalogue creation, system checks whether OEM for the brand mentioned in the catalogue exists on GeM or no. In case an OEM is registered, the approval request is routed to the OEM, otherwise it is sent to product approval team for review and approval		request accordingly
		1.2	Catalogue moves to Waiting for Admin Approval or Waiting for OEM Approval tabs respectively
2	OEM/ Product Approval team reviews the catalogue, and validates the information provided by the Seller (e.g., MRP proof, etc.). In case everything is in order, the catalogue gets approved and goes live on the GeM portal	2.1	Notification via email and portal
		2.2	Catalogue published on GeM and moved to Published tab
		2.3	Catalogue mapped to respective category, and unique combination of brand and golden parameters
3	In case the information is incorrect/ inappropriate then the catalogue request is rejected, and the Seller needs to create a new catalogue with appropriate details and submit it for approval again	3.1	Notification via email and portal
4	In case most of the information provided by the Seller is appropriate, and there are only a few discrepancies, the approver notifies the Seller and provides suggestions against relevant fields. In this case, Seller can edit the catalogue and re-submit for approval	4.1	Notification via email and portal
		4.2	Catalogue moved to Notified tab. Seller can edit catalogue as per suggestions provided by approval team/ OEM and resubmit for approval

Table 38: Products Catalogue Approval process and functionalities

Catalogue Edit/ Modification

Once the catalogue is published, individual Sellers can edit details directly associated with them in the catalogue – e.g., stock details, location, minimum order quantity, delivery locations serviced, Make in India component, MRP, offer price, discounts on the products, etc. No approval is required in this case and the modified details are then reflected on the GeM portal.

In case of a 'Notified' catalogue, Sellers can edit the catalogue and re-submit for approval, for publishing on GeM.

Sellers, both OEM and resellers, also have the option to discontinue a catalogue. If a reseller discontinues a particular catalogue, it is only discontinued for them. Whereas if an OEM discontinues a catalogue, it is discontinued for both the OEM as well as its resellers. Discontinued catalogue cannot be revived. Also, it cannot be re-uploaded by Seller/ OEM.

The process flow for product catalogue editing/modification is depicted below:
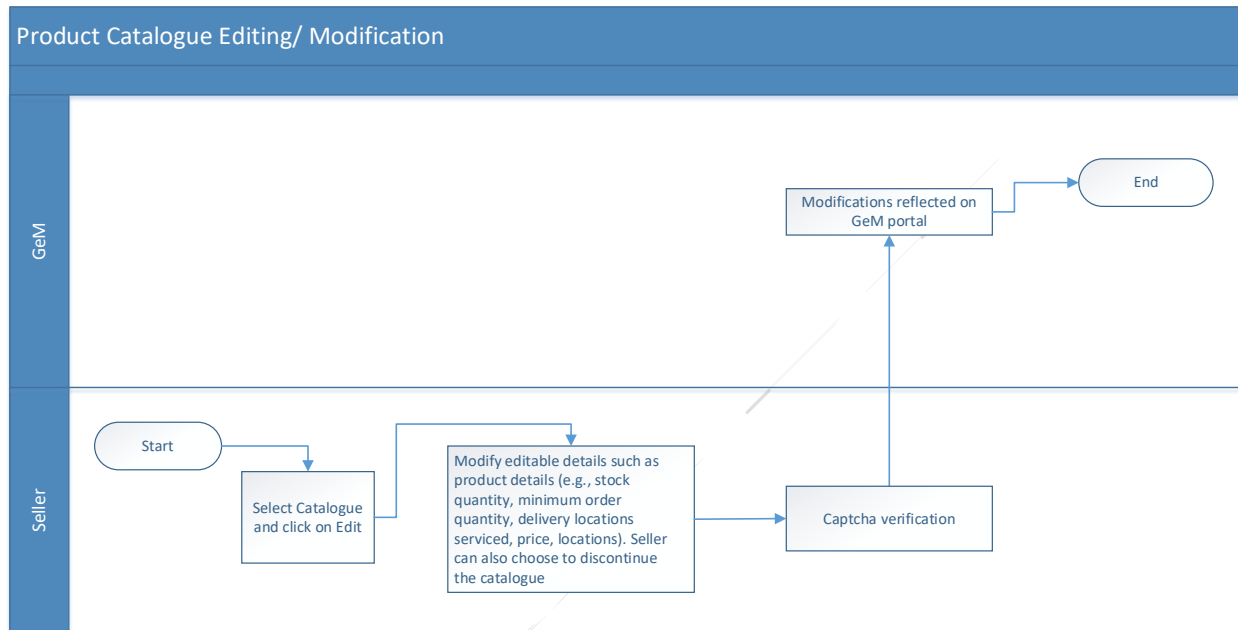
Figure 15: Product Catalogue Edit/ Modification

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Seller selects the catalogue and clicks on Edit		
2	Seller edits the relevant, Seller-specific product details (e.g., stock quantity, minimum order quantity, delivery locations serviced, price, locations) Seller can also choose to discontinue the catalogue	2.1	Only certain fields to be editable by Sellers
		2.2	Removal of catalogue from GeM in case of discontinuation by OEM

3	Once the edits have been made, Seller verifies via captcha code generated and submits the changes	3.1	Captcha generation and validation via input
4	Post submission, the changes get reflected on the GeM portal	4.1	Revised catalogue published on GeM

Table 39: Product Catalogue Edit/ Modification process and functionalities

New Brand Creation

In case a brand that Seller searched for is not available on GeM, he/ she can apply for the creation of a new brand. This request can accompany a request for OEM panel as well if the Seller declares themselves to be an OEM of the brand at the start of the process.

A brand can be of three types:

1. Registered

2. Unregistered

3. Unbranded

For unregistered and unbranded brands, only OEM can apply for brand creation. Once the brand is approved, resellers can then select the brand and upload their catalogues.

In case of registered brands, OEM and resellers both can apply to create a brand. In case a reseller has already created a registered brand on GeM, and the brand OEM registers on GeM later, the OEM can choose to either pair or discontinue all catalogues pertaining to that brand.

The process flow for new brand creation and approval is depicted below:
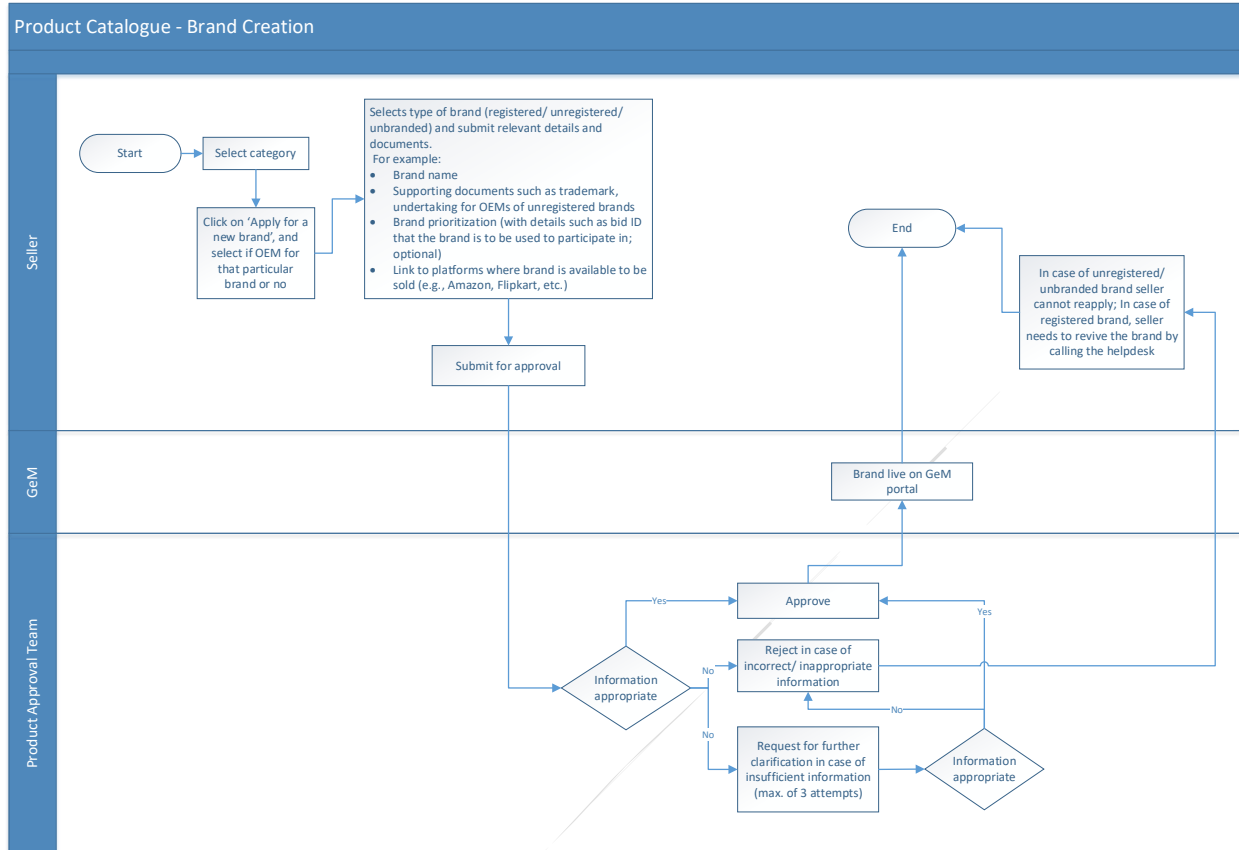
Figure 16: Brand Creation

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Seller selects category and clicks on apply for a new brand, and selects if he/ she is the OEM for that particular brand or no	1.1	Category search functionality
2	Post this, Seller selects the type of brand (registered/ unregistered/ unbranded) and submits the relevant details and documents. For example: 1. Brand name	2.1	Document upload functionality and storage on cloud
		2.2	Defined algorithm to manage incoming queue for brand approval from multiple Sellers.

	2. Supporting documents such as
	   a. For registered brand, "Trademark certificate" is required
	   b. For Unregistered brand, Undertaking from OEM on the stamp paper will be accepted
	   c. For unbranded, "Any Government Order copy" is required
	3. Brand prioritization (with details such as bid ID that the brand is to be used to participate in; optional)
	4. Link to platforms where brand is available to be sold (e.g., Amazon, Flipkart, etc.)
			This algorithm adjusts priority on the basis of various parameters like a brand for ongoing bid, a brand for Covid-19 related categories, etc.

3	Once these details have been provided by the Seller, the brand creation request goes to the product approval team	3.1	Workflows to re-route request to appropriate teams
4	In case the information is appropriate, product approval team approves the brand, post which the brand becomes live on GeM portal	4.1	Brand reflected on GeM portal
		4.2	OEM panel access granted in case the Seller is the brand OEM
5	In case the information is insufficient, the approval team can request for more information from the Seller. The approval team will have 3 attempts to seek further information post which they will have to either approve or reject the brand/ brand request	5.1	Mandatory approve/ reject choice to approver once the 3 attempts to seek further clarifications are exhausted
6	In case the information is incorrect, the product approval team rejects the brand or a particular request w.r.t that brand from a reseller. In case a brand is rejected then the Seller cannot re-apply to create the same brand. In case of registered brand, Seller will have to email/ call the helpdesk to get the brand revived from		

Table 40: Brand creation and approval process and functionalities

8.1.5.2   Services Catalogue Management

The Catalogue Management System enables the Service Providers to broadcast their services, rate sheets and introduce new services.
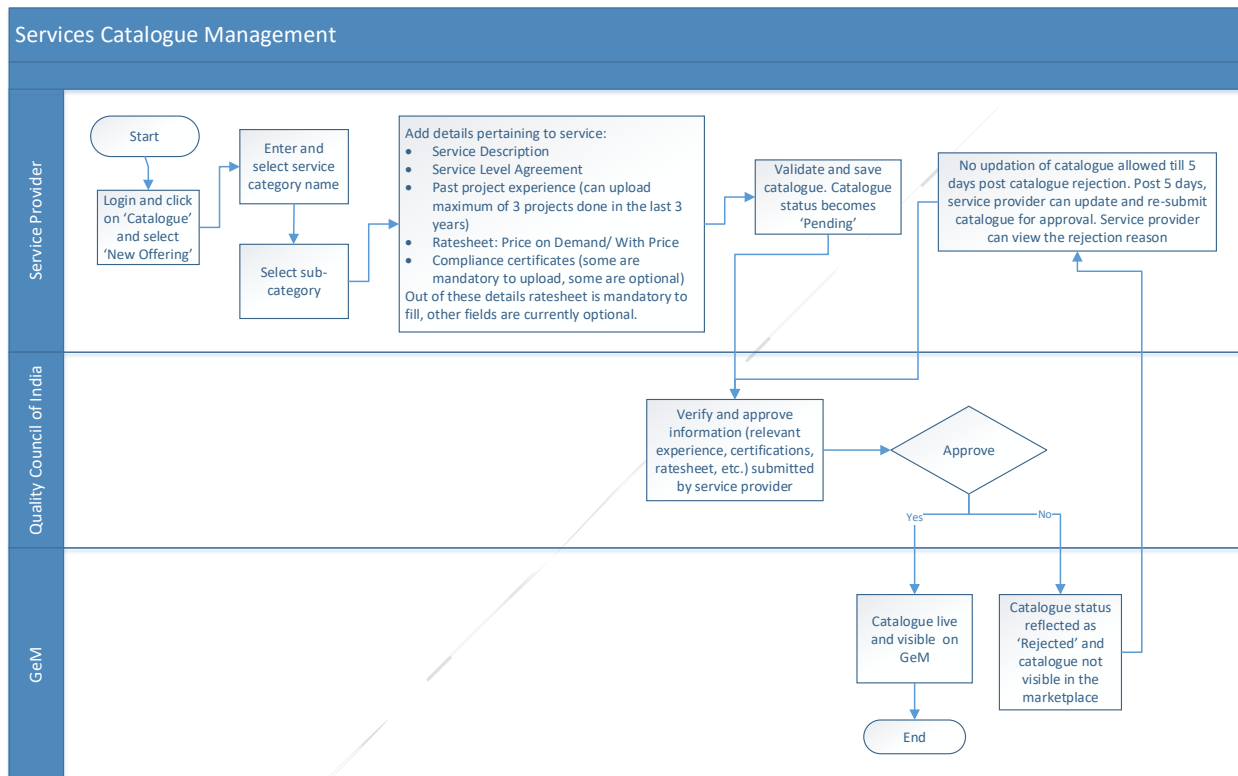
Figure 17: Services Catalogue Management

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Service provider logs in, clicks on 'Catalogue' and selects 'Add New Offering'		

2	Service provider types the service category name in which he/she wants to upload catalogue into	2.1	Name suggestions by the system in a drop-down form as Service Provider types the name
3	He/she can then view the sub-categories mapped to the category selected. Service provider selects the appropriate sub-category	3.1	Sub-category to category mapping

4	Service provider then adds following service details:
	
	1. Service Description
	2. Service Level Agreement
	3. Past project experience (can upload maximum of 3 projects done in the last 3 years)
	4. Rate sheet: Features 2 options
	   a. Price on Demand: Service provider submits the price at a later stage based on bid requirements
	   b. With Price: Service provider enter details such as minimum and maximum quantity he/ she can serve, price, etc.
	5. Compliance certificates (some are mandatory to upload, some are optional)
	
	Out of these fields, rate sheet is mandatory to fill, while others are currently optional.
		4.1	Document upload functionality and storage on cloud

		4.2	Rule engine to ensure <=3 projects done in the last 3 years have been added
		4.3	Integration with FSSAI
		4.4	Category related service configuration options for rate sheet visible. Service provider can select the ones applicable.
5	Service provider validates and saves catalogue	5.1	Functionality to enable digital signature / e-Sign based authentication
		5.2	Trigger OTP for verification to Service Provider & verify using the input
6	The details provided by Service Provider are then verified by a Third Party Agency (currently Quality Council of India (QCI)) (Rate sheet is sent/ not sent for approval	6.1	Post approval, catalogue mapped to relevant sub-category and category and made live on GeM portal
		6.2	Status update on GeM as 'Approved' or

depending on category rules). In case they are verified, catalogue is approved and made visible in GeM marketplace. In case it is rejected, the catalogue status gets updated to 'Rejected' on GeM portal. He/ she can update the same within 5 days and re-submit for approval		'Pending' as per catalogue status
	6.3	Email notifications to Service Providers upon approval/ rejection of catalogue

Table 41: Services Catalogue Management process and functionalities

8.1.5.3 Additional interventions/ functionalities needed:

Product Catalogue Management

1. Digitization of sub-processes, e.g., automated verification and authorization of data and documents provided, to minimize manual effort and improve speed of catalogue upload to GeM portal should be done

2. Additional role of checker or reviewer is required to be developed in the GeM system *(currently ongoing)*

3. Macro-based, bulk upload of catalogues via upload of an Excel sheet containing details of multiple catalogues in a pre-defined format should be enabled.

4. Integrations such as HSN code integration will be required as GeM scales its operations in the future

5. Data fields to provide details around HSN and GST percentage on a particular product should be given *(currently ongoing)*

6. Functionality to capture base price/ MRP and GST percentage on a product separately

7. Functionality to manage product variants and related variations in product parameters such as multiple price points based on product variant, location, etc., with the option to link product videos/ demos, should be provided.

8. Provision for regular revision and confirmation of the MRP

Services Catalogue Management

1. In case Service Provider only provides the rate sheet and not the relevant experience and certifications, GeM auto-approves the category without need for QCI approval for certain

services categories. This process needs to be modified to prevent auto-approval of services catalogues

2. Need for a GeM facing, real-time dashboard highlighting the volume of catalogue approval requests with QCI, their status, reason for rejection, and other key metrics, to enable GeM to oversee the catalogue approval process

3. Functionality for QCI or other inspection agencies to verify project completion status & other details quoted by Service Providers within 'Relevant Experience' via GeM database & systems, in case the project contract was awarded via GeM

4. Need for a specific experience criterion for Service Providers depending on service category, bid value and other key parameters. E.g., for an INR 1 Cr bid, Service Provider should either mention 1 project worth INR 80 Lacs, or 2 projects worth INR 50 Lacs each, or 3 projects of 40 Lacs each done in the past 3 years

5. Scope for improvement in the user interface for rate sheet section. Potential to explore uploading of rate sheet via excel based format with drop down option. Service provider can fill and upload the same to the portal

6. Rate sheet download functionality to enable Service Providers to modify prices and upload the same to GeM

7. Multiple rate sheets within the Service, e.g., Price per month per vehicle, Price per Driver per Month.

8. Provision to mention base price and GST breakup separately while uploading the catalogue, and price quotation during bid participation

9. Currently the status of a catalogue is only visible after clicking the respective catalogue. Status (Approved/ Pending) should be shown right next to the catalogue. This can be done by adding a colour-coded banner stating Approved/ Pending against each catalogue

10. Add a data field to enable Service Providers to highlight if they are an empaneled Service Provider. If yes, allow them to provide further details around which service are they empaneled for, with which Buyers, etc. The information then can be verified by QCI

11. View/ Update catalogue option is currently not active for services. These options need to be activated

12. Provision to upload service catalogues in bulk through Excel

13. Provision to download catalogue in excel, modify it and re-upload it

14. Service provider should be allowed to decrease the price anytime but can increase the price not before 15 days of updation

15. Service provider should be allowed to migrate or copy the offering from 1 service to another service with modifications

16. Functionality to enable Original Service Provider (OSP) to register themselves as OSP, register their brand, map and authorize resellers within service category (e.g., Cloud Services), and approve service catalogues uploaded by resellers *(currently ongoing)*

17. OSP-Reseller mapping functionality required

8.1.6   E-Procurement

Overall e-procurement process at GeM comprises of various processes – direct purchase, Lowest cost purchase (L1 buying), category-led bid and reverse auction, custom bid, BoQ bid and Forward auction. Apart from these processes, GeM has also recently introduced additional procurement methods such as push button procurement. This section offers a detailed view of the e-procurement process as a whole and is followed by sub-sections explaining the individual processes in detail.

While all the current processes and workflows have been indicatively captured in this section of this RFP, it should be noted that there may be certain changes in these e-procurement processes and workflows as a result of ongoing development of features & functionalities in the period between release of this RFP and MSP onboarding or as an outcome of ministerial guidelines impacting the scope of GeM (e.g., onboarding of cooperatives, etc.). Hence final business implementation should be as per the requirements finalized and documentation (BRD, FRS, SRS, HLD, LLD, system architecture, etc.) approved during the design phase as mentioned in Implementation Schedule in this RFP.
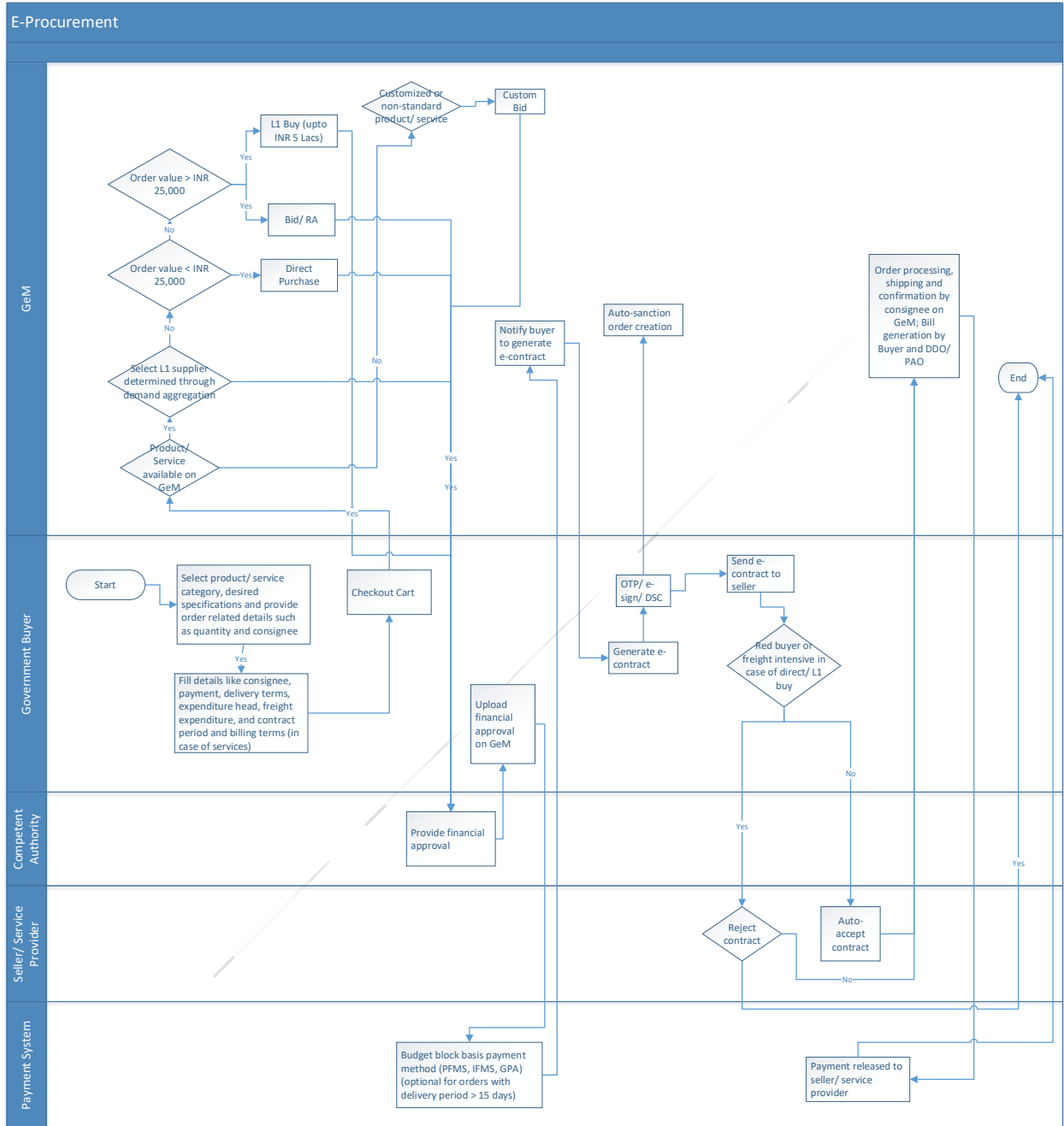
Figure 18: E-procurement Process

8.1.6.1 Direct Purchase

Buyers can purchase products/ services directly on GeM in a one-click fashion up to a threshold value. Currently, this threshold value is setup at INR 25,000 for all Buyer organizations. Select automobile categories such as cars, trucks, buses, etc. and some drugs categories are exempted from this INR 25000 ceiling for direct purchase currently.
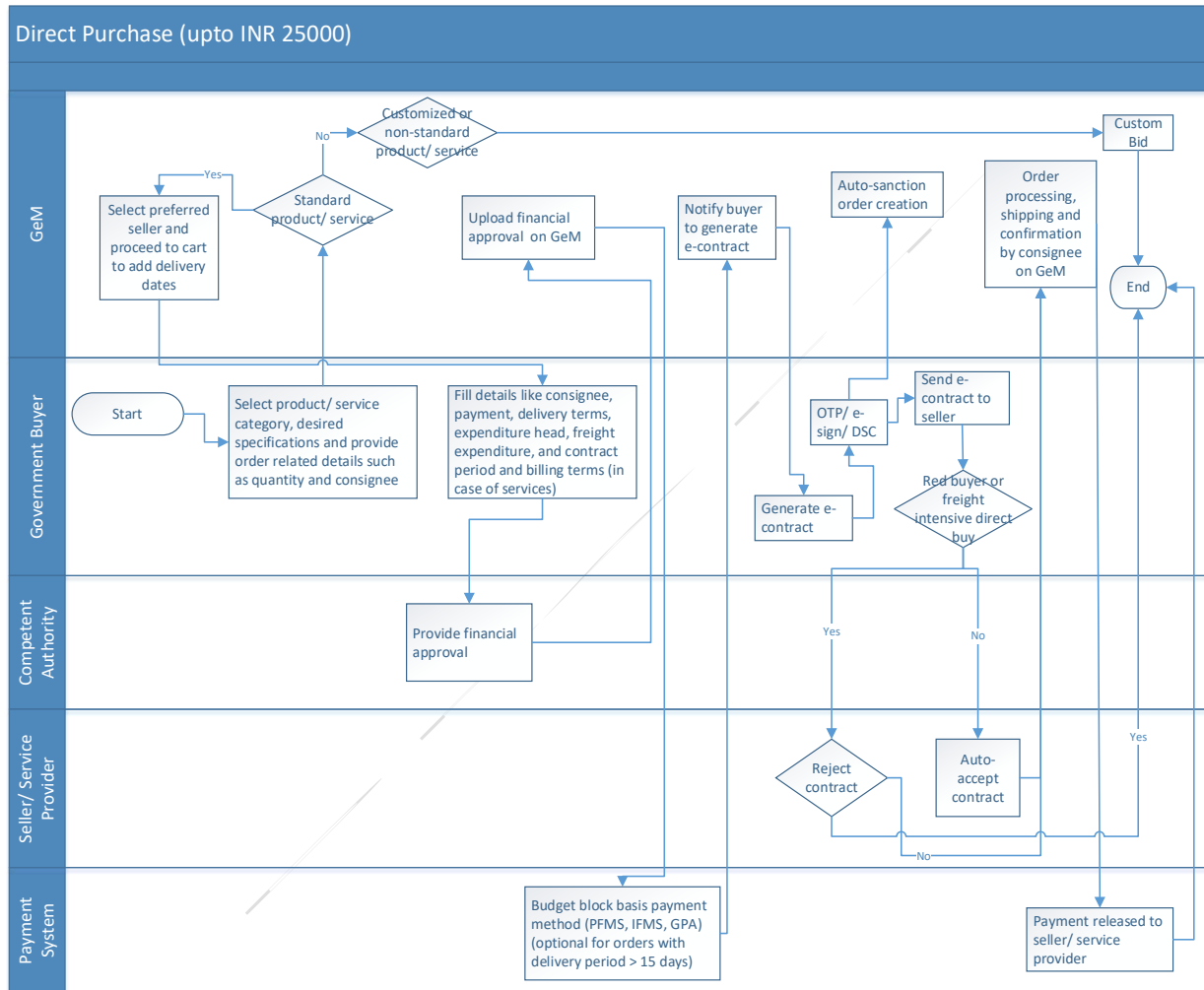
Figure 19: Direct Purchase Process

Detailed Process Flows				
#	**Process Steps**	**#**	**System Functionality**	
1	The Buyer selects product/ service category, desired specifications, and provide order related details such as quantity, consignee, etc.	1.1	Product/ Service catalogue search functionality	
		1.2	Automated products/ services catalogue filtration basis selected consignee location	

2	In case it is a standard product/ service and is available, Buyer selects product/service and proceeds to cart. At this stage, the Buyer needs to provide additional details such as
	   1. Consignee
	   2. Payment details
	   3. Delivery terms
	   4. Expenditure head
	   5. Freight expenditure
	   6. Contract period (in case of services)
	And any other details, as configured by category owner			

3	Buyer gets financial approval for the purchase from competent authority and uploads the same on GeM and blocks the budget	3.1	Collected documents stored on cloud	
		3.2	Integration with PFMS, IFMS, GPA	
4	Buyer gets a notification to generate e-Contract	4.1	Automated notification to Buyer on the portal, and via e-mail and SMS	
5	Buyer generates e-Contract and validates it via OTP/ e-sign/ DSC, post which a sanction order is created	5.1	Functionality to enable digital signature / e-Sign based authentication	
		5.2	Trigger OTP for verification to Buyer & verify using the input	
		5.3	Auto-sanction order creation by GeM portal	
6	Buyer sends the e-contract to Seller/ Service Provider. If the Buyer is not a 'red Buyer' (Buyers with pending payment for 30 or more orders from more than 70 days of CRAC) and	6.1	System triggered auto-acceptance or Seller triggered rejection of contract based on defined rules	

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	contract doesn't involve purchase of freight intensive categories (e.g., automobile – has 10 sub-categories), the system auto-accepts the contract. In case of red Buyers and freight intensive categories, the Seller can reject the contract		
7	Post acceptance of contract, order is processed and fulfilled by Seller. Proof of delivery is uploaded by the Seller on GeM portal, post which consignee provides confirmation via PRC and CRAC/ SDAC (in case of services)		To be covered in detail in Order Fulfilment section
8	Post Buyer confirmation, invoice is generated, and payment is released to the Seller. GeM receives payment status and displays it on the portal. Service providers have the option to raise multiple invoices.	8.1	Integration with PFMS, IFMS, GPA
		8.2	Payment status displayed on GeM

Table 42: Direct Purchase Process & Functionalities

8.1.6.2   Lowest Cost Buying (L1 Buy)

Buyers can purchase products/ services via L1 Buy on GeM up to a threshold value. Currently, this threshold value is setup at INR5 Lacs for all Buyer organizations. Select automobile categories such as cars, trucks, buses, etc. are exempted from this ceiling for L1 Buy currently.

In this method, the Buyer has to select and compare the prices from 3 Sellers/ Service Providers offering the desired product/ service mandatorily before placing the order. Once, the Buyer selects the three different brands from three different Sellers in case of product or three different Service Providers, the system compares the selected Sellers as well as other Sellers offering the desired product and recommends a L1 Seller. The Buyer can choose to proceed with the system recommended L1 Seller or create a bid.
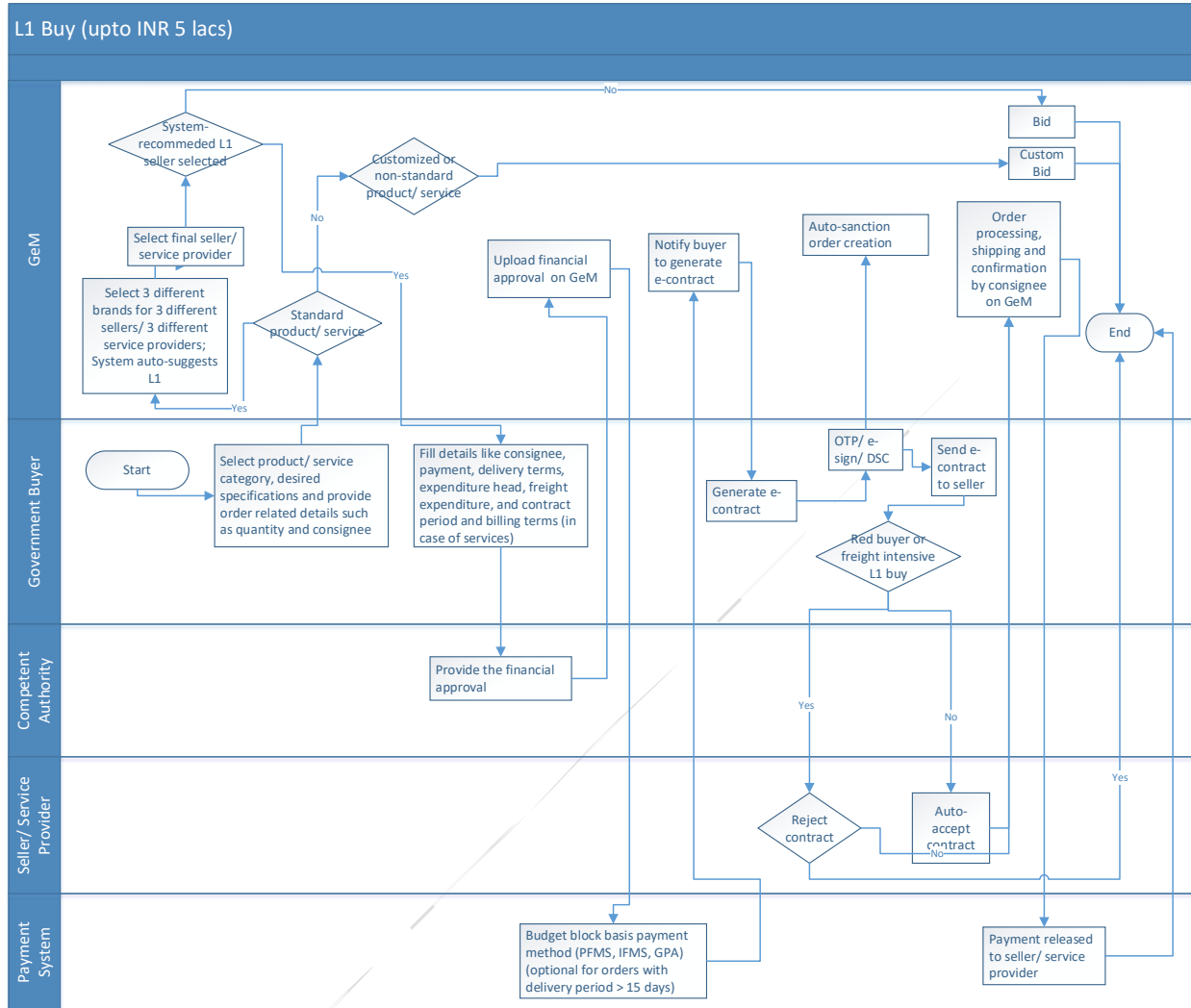
Figure 20: L1 Buy Process

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1		1.1	Product/ Service catalogue search functionality

Detailed Process Flows

#	Process Steps	#	System Functionality
	The Buyer selects product/ service category, desired specifications, and provide order related details such as quantity, consignee, etc.	1.2	Automated products/ services catalogue filtration basis selected consignee location
2	In case it is a standard product/ service and is available, Buyer selects three different brands from three different Sellers in case of product or three different Service Providers offering the desired product/ service. Post this the system compares the selected Sellers as well as other Sellers in the system and auto-displays the L1 Seller/ Service Provider. In case, system recommended L1 is one of the 3 Sellers/ Service Providers selected by the Buyer and Buyer chooses to proceed with the system recommended L1, he/ she can proceed with L1 buy. Otherwise, the Buyer will have to create a bid	2.1	Auto-comparison and recommendation of L1 Seller/ Service Provider for desired product/ service basis selected golden parameters
3	Buyer selects system recommended L1 Seller/ Service Provider and proceeds to cart. At this stage, Buyer needs to provide additional details such as 1. Consignee 2. Payment details 3. Delivery terms 4. Expenditure head 5. Freight expenditure 6. Contract Period		
4	Buyer gets financial approval for the purchase from competent authority and uploads the same on GeM and blocks the budget	4.1	Collected documents stored on cloud
		4.2	Integration with PFMS, IFMS, GPA
5	Buyer gets a notification to generate e-Contract	5.1	Automated notification to Buyer on the portal and via e-mail
6	Buyer generates e-Contract and validates it via OTP/ e-sign/ DSC, post which a sanction order	7.1	Functionality to enable digital signature / e-Sign based authentication

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	is created, and purchase order no. is assigned by the system	7.2	Trigger OTP for verification to Buyer & verify using the input
		7.3	Purchase Order No. generation and auto-sanction order creation by GeM portal
7	Buyer sends the e-contract to Seller/ Service Provider. If the Buyer is not a 'red Buyer' and contract doesn't involve purchase of freight intensive categories (e.g., automobile), the system auto-accepts the contract. In case of red Buyers and freight intensive categories, the Seller can reject the contract	7.1	System triggered auto-acceptance or Seller triggered rejection of contract based on defined rules
8	Post acceptance of contract, order is processed and fulfilled by Seller. Proof of delivery is uploaded by the Seller on GeM portal, post which consignee provides confirmation via PRC and CRAC		To be covered in detail in Order Fulfilment section
9	Post Buyer confirmation, payment is released to the Seller. GeM receives payment status and displays it on the portal	9.1	Integration with PFMS, IFMS, GPA
		9.2	Payment status displayed on GeM

Table 43: L1 buy process & functionalities

8.1.6.3   Bids/ Reverse Auction

Any product or service worth greater than a threshold value as defined by GeM, are mandatory to be procured through Bid/ RA method. Currently, this threshold value is setup at INR 5,00,000 for all Buyer organizations. Products and services below INR 5,00,000 can also be procured via bidding and RA method, basis Buyer discretion. Procurement through bidding and RA method mainly includes three key process steps:

1. Bid/ RA creation by the Buyer

2. Participation by the Sellers / Service Providers

3. Evaluation and award process (Bid to RA functionality is available for use at this stage to drive higher cost efficiency)

Different types of bids can be floated based on requirement:

1. Category based product/service bid

2. Custom bid – In case category or product/ service specifications are not available on GeM

3. BOQ bid

4. PAC bid - If any Buyer wants to purchase a particular Brand/ Model of any product, then the Buyer has to obtain a 'Proprietary Article Certificate' (PAC) from the competent authority of the Buyer's organization and make procurement through 'PAC Buying' option available on GeM Portal

Apart from various types of bids, GeM also features specific provisions such as the ones detailed below to enhance ease of procurement:

1. Installation commissioning and testing feature (ICT): Buyers have the feature to capture prices of Installation, Commissioning & Testing separately in Bid to ensure that payments are made according to the milestone completed by the Seller. Sellers may get a part of their product cost alone on supply and remaining part on completion of Installation, Commissioning and Testing. Buyer may also opt for Incidentals such as Training, Statuary Compliances, etc. which may be paid as per their milestones.

2. Input Tax Credit (ITC): Input Tax Credit is required by Buyers who are eligible for Input Tax Credit on GST and GST cess (wherever applicable) in their purchase. Since they get credit of GST therefore, they require financial evaluation of Bid considering input tax credit (ITC) so that L1 evaluation is on net landed cost to the Buyer. There are three types of Sellers/ Service Providers in this case - regular GST registered, unregistered, and those registered under composition scheme. Bid L1 evaluation is based on Input Tax Credit Available and Reverse Charge Mechanism (in case of procurement from unregistered Seller/ Service Provider and from registered Seller/ Service Provider where categories of goods and services have been notified under sections 9(3)). The Buyer may specify the % of GST and GST cess details (wherever applicable) and percentage of ITC on GST and GST cess which is available as Input Tax Credit to the Buyer.

3. Annual Maintenance Contract (AMC)/ Comprehensive Maintenance Contract (CMC): An AMC is an agreement with a Service Provider/supplier/manufacturer for providing technical support to inspect, repair and maintenance of product/equipment/machinery for mutually agreed period of time. Once the warranty period expires of any product, AMC takes care of its maintenance to keep it in working condition. AMC generally involves preventive maintenance support without involving the cost of replacements.

4. A CMC is an agreement with a Service Provider/supplier/manufacturer for providing technical support to inspect, repair and maintenance of product/equipment/machinery including cost of spares, replacements and labor charges for mutually agreed period of time. CMC generally take care of the responsibility to keep the product/equipment/machinery in good working order, regardless of any factor, subjected to any exception in the contract.

5. Price Variation Clauses: Price Variation Clauses (PVC) are used in settling claims between Buyer and Seller for variation in the basic price of raw materials from the period of Bidding till the date of delivery. These clauses are widely accepted by the industry and purchasing organizations, since they give variations on both sides, either upwards or downwards. By substituting the prices of raw materials in the given formulae appropriately the percentage variation over quoted price can be worked out mathematically

6. Bid Evaluation Methods: GeM features multiple bid evaluation methods in case of bunching of items in bids and BoQ. These include total value wise evaluation, item-wise evaluation, consignee wise evaluation, group wise evaluation in case Buyer wants to schedule items into groups. Earlier GeM Buyers used to get Seller offers against items for pre-defined consignee locations, which were evaluated for total cost offered. Now with item wise and consignee wise evaluations, Sellers can offer rates along multiple dimensions. For example, Buyer may like to know what Seller offer would be for a specific consignee location for an item instead of for all locations. This helps the Buyer to get best value.

Bid/ Direct RA Creation:

Following is the process for bid/ Direct RA creation:

Buyer

Start

Search for desired product or service, select required specifications, golden and non-golden parameters, input consignee details, and add to cart (Items/ services in the cart can be bunched with same or different categories)

Select procurement mode as bid or RA mode (other modes available – PAC, etc.) and enter bid/ RA details such as:
- Bid lifecycle (start date, bid duration, offer validity, etc.)
- Bid qualification and evaluation criteria (pre-qualification, technical evaluation, evaluation method – QCBS/ LCS, etc.)
- Documents to be uploaded by bid participants
- Bid to RA option – Yes / No (only available in case of Bid and not Direct RA)
- In case Bid to RA is yes - Method for RA qualification (50% qualified bidders move to RA/ H1 bidder gets eliminated)
- Add multiple consignees
- Pre bid meeting (optional)
- Additional service specific details (Financial breakup, bid estimated value, floor price, payment terms, contract duration, etc.)
- Upload of drawings and scope of work in case of engineered goods
- Staggered delivery plan mapped to quantities and consignees
- Bid Reference Price
- Time to be allowed to seller/ service provider to respond to Technical Clarifications raised by buyer during technical evaluation phase
- Buyback option and form

Select if EMD or e-PBG clause is applicable- add advisory bank, define percentages and duration,etc. (Option available for bid value > INR 5,00,000 and is optional)

Select from multiple features or functionalities available such as:
- No. of sellers to be awarded
- Bid/ Direct RA splitting (e.g., partial quantity distribution across multiple sellers, no. of bidders, criteria)
- Govt. policies compliance features such as Make in India (MII) %, MSE %, etc. (If buyer bypasses MII then CA approval upload – for bids ranging between INR 5 Lakhs to INR 200 Cr)

Add Additional Terms & Conditions (ATCs) for the bid such as certification documents required (availability of static and dynamic ATCs), scope of work and service levels (SLAs) in case of services, inspection method, etc.

OTP/ e-sign/ DSC verification for bid/ Direct RA creation

GeM

Publish bid (including buyback details)/ Direct RA

Notify prospective sellers/ service providers via automated e-mail, SMS

End

Figure 21: Bid/ Direct RA Creation

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyer searches for desired product or service, select required specifications (golden parameters – core parameters for the product/ service that also govern the price variation within products of the same categories), input consignee details, and adds product/ service to cart Buyer can also add (up to 5) parameters for specification along with existing item parameters captured on GeM. During this step the price of the product selected is captured and can be shared by the Buyer as Bid Reference Price in the Bid Document during the bid creation stage	1.1	Interaction between category management, search and bid modules
2	Buyer selects procurement mode as bid/ RA mode (Buyer also has the option to procure via direct purchase, given cart value) and enter details such as: 1. Bid lifecycle (start date, bid duration, offer validity, etc.) 2. Bid qualification and evaluation criteria (pre-qualification, technical evaluation, evaluation method – QCBS/ LCS, etc.) 3. Documents to be uploaded by bid participants (including Financial document with prices of spares and consumables) 4. Bid to RA option – Yes / No (only in case of bid creation and not for Direct RA) 5. In case Bid to RA is yes - Method for RA qualification (50% qualified bidders move to RA/ H1 bidder gets eliminated)	2.1	Information on key parameters such as bid opening date, etc. stored and used to implement system-triggered guardrails. For e.g., bid not allowed to be open prior to set open date
		2.2	Upload and cloud-based storage features for all the documents as defined in the bid

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	6. Add multiple consignees		
	7. Pre bid meeting (optional)		
	8. Additional service specific details (Financial breakup, bid estimated value, floor price, payment terms, contract duration, etc.)		
	9. Upload drawings and scope of work in case of engineered goods		
	10. Staggered delivery plan mapped to quantities and consignees		
	11. Time to be allowed to Seller/ Service Provider to respond to Technical Clarifications raised by Buyer during technical evaluation phase		
	12. Buyback option and form (GeM has provided a Buyback option to its user through which the Buyer will be able to procure new goods and dispose off old goods. The Seller will quote the price of new goods along with the price offered for old goods as buy back; At present Buyback option is enabled in 37 categories). In case Buyer selects buyback as 'Yes' then he/ she is required to fill the buyback form capturing the item details & description, model no., brand, purchase date, quantity, images, etc.		
3	Buyer selects if an EMD or e-PBG clause is applicable in the concerned bid. This option is only available for bid value greater than INR 5,00,000 and is optional	3.1	Upload and cloud-based storage features for all the documents as defined in the bid

Detailed Process Flows			
#	Process Steps	#	System Functionality
4	Buyer selects from multiple features or functionalities available such as: 1. No. of Sellers to be awarded 2. Bid/ RA splitting (e.g., partial quantity distribution across multiple Sellers) 3. Govt. policies compliance features such as Make in India (MII) %, MSE %, etc.)	4.1	Availability of all required features with system-based interlocks or guardrails during bid evaluation stage
5	Buyer adds Additional Terms & Conditions (ATCs) for the bid such as certification documents required, scope of work and service levels (SLAs) in case of services, inspection method, etc.	5.1	Pre-defined ATCs available for Buyers to select and elaborate upon with option to add specific additional terms
6	Buyer verifies the bid/ RA creation and draft bid/ RA document via OTP/ e-sign/ DSC verification	6.1	Functionality to enable digital signature / e-Sign based authentication
		6.2	Trigger OTP for verification to Buyer & verify using the input
		6.3	Bid Document creation and publishing
7	Bid/ RA is published on GeM portal, along with Bid Document including Buyback details if applicable, and all existing Sellers/ Service Providers within selected category are notified automatically, through e-mail and SMS. Sellers/ Service Providers can refer to the bid document	7.1	Interaction between category, Seller management and bid modules
		7.2	Automated emails and SMS to notify prospective Sellers/ Service Providers of the bid

Table 44: Bid/ Direct RA Creation process and functionalities

Bid Participation:

All eligible and interested Sellers / Service Providers have option to raise representation or clarifications as needed on the details mentioned in the bid created. Buyer is required to address and

revert to all representations or clarifications raised by Sellers and create a bid corrigendum before bid participation is opened. For bid participation, each Seller/ Service Provider either selects from their existing product/ service catalogues or uploads a new catalogue basis bid requirements and specifications.

Bid participation cannot be closed unless all representations have been responded and addressed in the system. Buyer must record his last reply at least 24 hours before bid end date and time. No representations will be allowed in last 72 hours of the bid end date and time.

If Buyer is recording his last reply with only 24 hours or less remaining for the Bid to end or after Bid End Date, Bid will have to be extended by 48 Hours minimum (Buyer can make it more) from the action date time and only can then proceed with Bid opening. Buyer will be prompted by system while submitting the response. If the Buyer himself does not extend, system would auto extend by 48 hours.
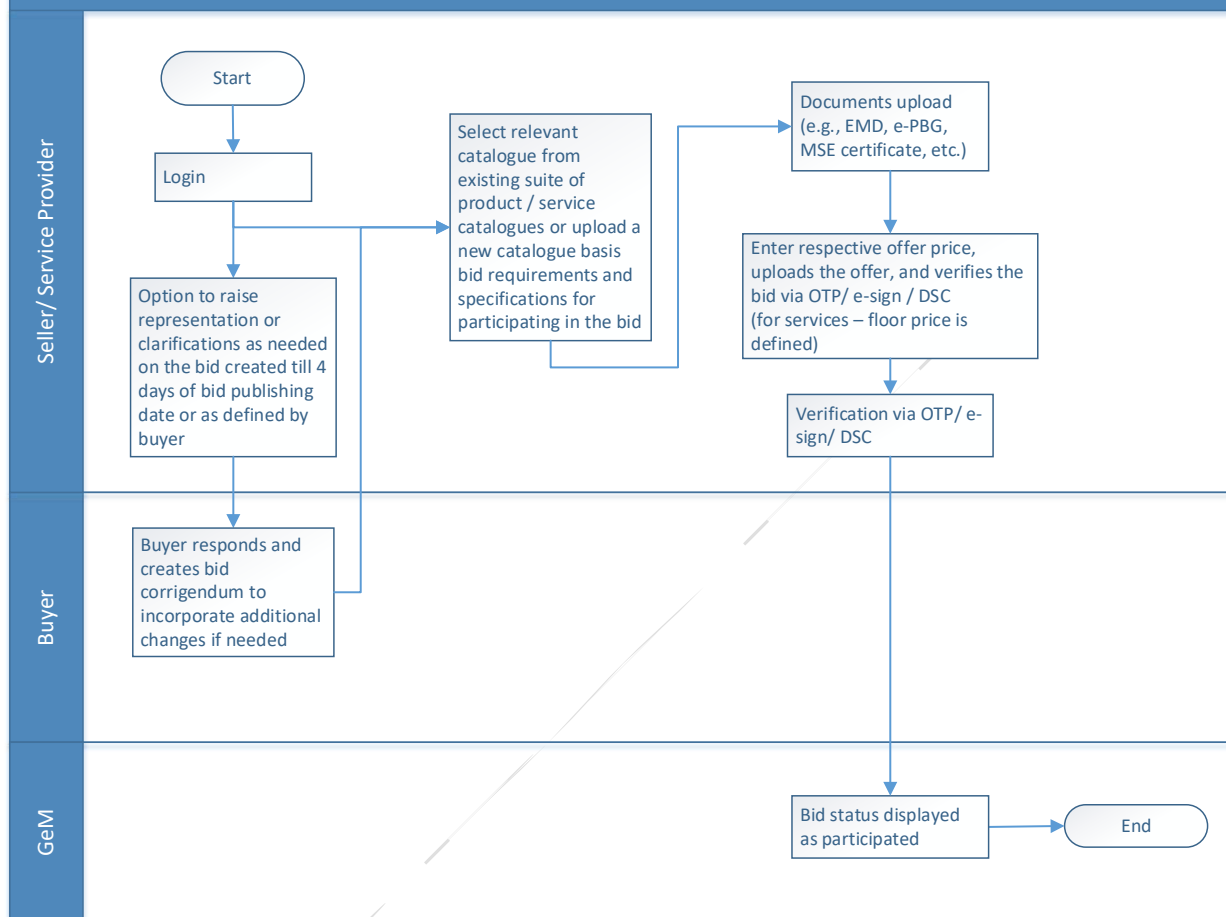
Figure 22: Bid Participation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Sellers / Service Providers have the option to raise representation or clarifications as needed on the bid created till 4 days of bid	1.1	Functionality to raise representations from Sellers and corrigendum addition

Detailed Process Flows

#	Process Steps	#	System Functionality
	publishing date or as defined by Buyer. Buyer addresses all representations and creates a bid corrigendum to incorporate additional changes to the bid if needed		from Buyer for defined timelines post bid publishing
2	Each Seller / Service Provider either selects from their existing suite of product / service catalogues or uploads a new catalogue basis bid requirements and specifications for participating in the bid	2.1	Functionality for Sellers / Service Providers to search for a specific bid on GeM portal basis different parameters such as Buyer name, type, bid no., etc.
		2.2	Interaction between catalogue management and bid modules
		2.3	Automated filling of available technical details from selected catalogue to bid
3	Seller/ Service Provider uploads additional required documents (e.g., EMD, e-PBG, MSE certificate, etc.)	3.1	Document uploading functionality. Store documents on cloud
4	Post this, each Seller/ Service Provider enters respective offer price and buyback price (if applicable), uploads the offer, and verifies the bid via OTP/ e-sign/ DSC	4.1	Functionality to enable digital signature / e-Sign based authentication
		4.2	Trigger OTP for verification to Buyer & verify using the input

Table 45: Bid Participation process and functionalities

Bid Evaluation:

Bid evaluation process consists of two types of evaluations: Technical and Financial.

The Buyer is able to open Technical Evaluation after the Bid End Time and once he responds to all representations submitted.

The Buyer has an option to review technical specification for each Seller submission. In technical evaluation, Buyer assesses and compares the technical specifications submitted by various Sellers / Service Providers participating in a bid. The offer comparison against reference product and allowed values is displayed to the Buyer for comparison purposes. The Buyer can also verify the documents uploaded by the Seller including the MSE certificate, etc.

Buyer has the option to seek clarifications, additional information / documents from participating Sellers/ Service Providers during technical evaluation, as many number of times as required.

Participating Sellers/ Service Providers are allowed a minimum of 48 hours or as more as defined by the Buyer to provide required clarification / information / document. Technical evaluation stage cannot be completed for all participating Sellers / Service Providers until all raised clarifications are addressed in the system from participating Sellers / Service Providers.

Post comparison, the Buyer should accept/reject each Seller offer providing reasons for each acceptance/rejection.

All disqualified Sellers are notified via their dashboard and email including reason for disqualification. Suspended and disabled Sellers are auto disqualified by the system.

In addition, post completion of technical evaluation, all participating Sellers / Service Providers are allowed to make any representations against disqualifications till 48 hours of the evaluation results publishing date and time. Buyer will have an option to Bypass this rejection / disqualification challenge buffer time i.e., 48 hours, only in bids with total defined duration less than 10 days by submitting an undertaking of the competent authority at Buyer end.

Post completion of rejection / disqualification challenge buffer time, financial bids can be opened in the system and system automatically displays the lowest cost or price bid (L1). In case the Buyer had selected the Bid to RA option as 'Yes' during the bid creation stage, the Buyer is mandated to initiate a RA process on the GeM portal. Post RA, Buyer has the option to further negotiate prices with L1 Seller / Service Provider. In case of bid splitting, system assesses the eligibility of a bid for price matching. In case the bid is eligible, Buyer is allowed to request L2 & L3 Sellers / Service Providers to match the L1 price. L2 & L3 Sellers/ Service Provider have an option to accept/ reject the same in system.

If more than one L1 is identified, the system will force for RA even though Buyer has not opted for Bid to RA as 'Yes'. In case no one participates in the RA then it comes to bid result where Buyer can choose any one L1 among multiple L1s identified.

Basis the final bid prices from various qualified Sellers/ Service Providers, Buyer finalizes the Seller(s) / Service Provider(s) and awards the bid.
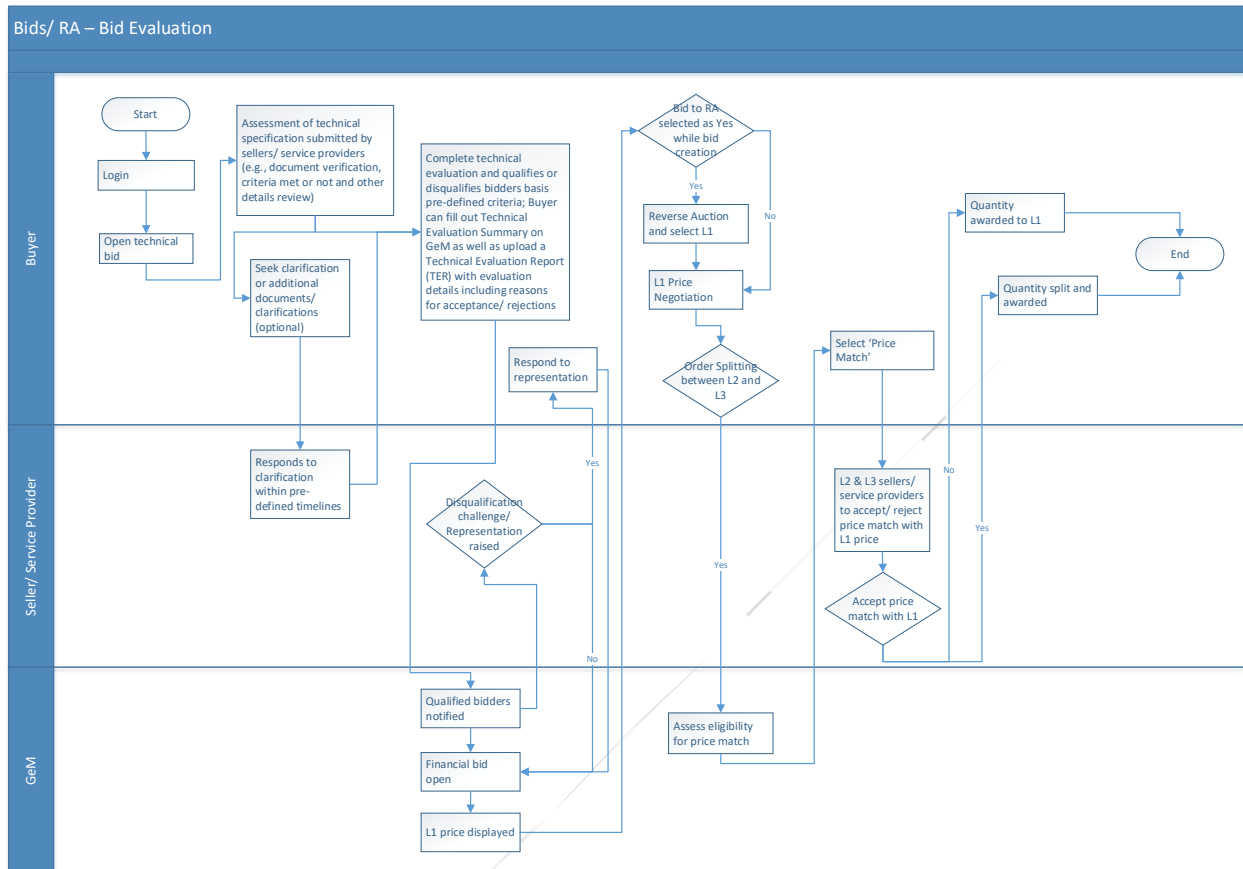
Figure 23: Bid Evaluation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Buyer opens technical bids of all participating Sellers / Service Providers and assesses the technical specifications submitted (e.g., document verification, criteria met or not and other details review)	1.1	Functionality for Buyers to score all participating Sellers / Service Providers against defined criteria for technical evaluation
2	If needed, Buyer can seek clarifications, additional information / documents from	2.1	Rule based bid freezing until defined timelines for participating Sellers /

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	participating Sellers/ Service Providers within defined timelines		Service Providers to respond to clarifications
3	Buyer completes technical evaluation and qualifies or disqualifies respective participating Sellers / Service Providers on the basis of pre-defined criteria in the bid	3.1	Automated notifications to technically qualified Sellers / Service Providers
	Buyer can fill out Technical Evaluation Summary on GeM. This helps the Buyer to make note of the technical evaluation within system itself, Buyer will be able to view the saved comments later during technical evaluation.	3.2	Functionality to upload Technical Evaluation Report for Buyers
		3.3	Provision to provide technical evaluation summary on GeM with functionality to auto-save and view comments later
	Buyer can also upload a Technical Evaluation Report (TER) with evaluation details including reasons for acceptance/ rejections		
4	Any participating Seller / Service Provider has the option to raise a disqualification challenge till 48 hours of the evaluation completion (24 hours in case of short bids – bids with a duration of less than 10 days) and Buyer needs to address the same within prior to opening the financial bid	4.1	Rule based bid freezing until defined timelines for Buyers to respond to disqualification challenge raised
5	Post challenges time is completed, financial bids are opened in the system and system automatically displays the lowest cost or price bid (L1). Buyer is also able to assess the buyback price of the Sellers/ Service Providers if applicable.	5.1	Automatic assessment and display of L1 price with Seller/ Service Provider name masked
6	If Bid to RA option is applicable, the Buyer is mandated to initiate a RA process on the GeM portal	6.1	Interaction between bid and RA modules
7	Once RA is completed, Buyer can further negotiate with L1 via negotiation feature available on the GeM system. Window for	7.1	Notification to L1 Seller when the Buyer initiates negotiation request
		7.2	Online negotiation functionality

Detailed Process Flows

#	Process Steps	#	System Functionality
	negotiation is open for 72 hours and a maximum of 5 attempts are allowed	7.3	Round wise price history details available for Buyer including initial price quoted by Seller/ Service Provider
8	In case of bid splitting, GeM assesses eligibility for price matching. In case the bid is eligible for the same, the Buyer can select price match option to request L2 and L3 Sellers to match L1 Seller price. L2 and L3 Seller can accept/ reject to match the price	8.1	Notification to L1 Seller when the Buyer initiates negotiation request
		8.2	Online feature to conduct up to 5 price negotiation rounds with L1 Seller / Service Provider
9	Bid is awarded to finalized Seller(s)/ Service Provider(s) and bid/ RA results are published on the portal	9.1	Award notification to selected Seller(s)/ Service Provider(s)

Table 46: Bid Evaluation process and functionalities

Bid to Reverse Auction (Bid to RA)

RA functionality can be used by the Buyer to drive higher cost efficiency. In this type of RA, eligible Sellers / Service Providers are shown the L1 price from the bid as reference and asked to input the revised prices they can offer basis the L1 price reference in multiple number of rounds. Sellers / Service Providers try to match or beat the L1 prices in subsequent rounds. Once the total desired number of rounds are completed or there is no new price offer in last 30 minutes of the RA, the system analyzes the bid results and publishes L1, L2 and L3 Sellers/ Service Providers. The Buyer can select the L1 Seller/ Service Provider and proceed with further negotiations.

Bids/ RA – Reverse Auction
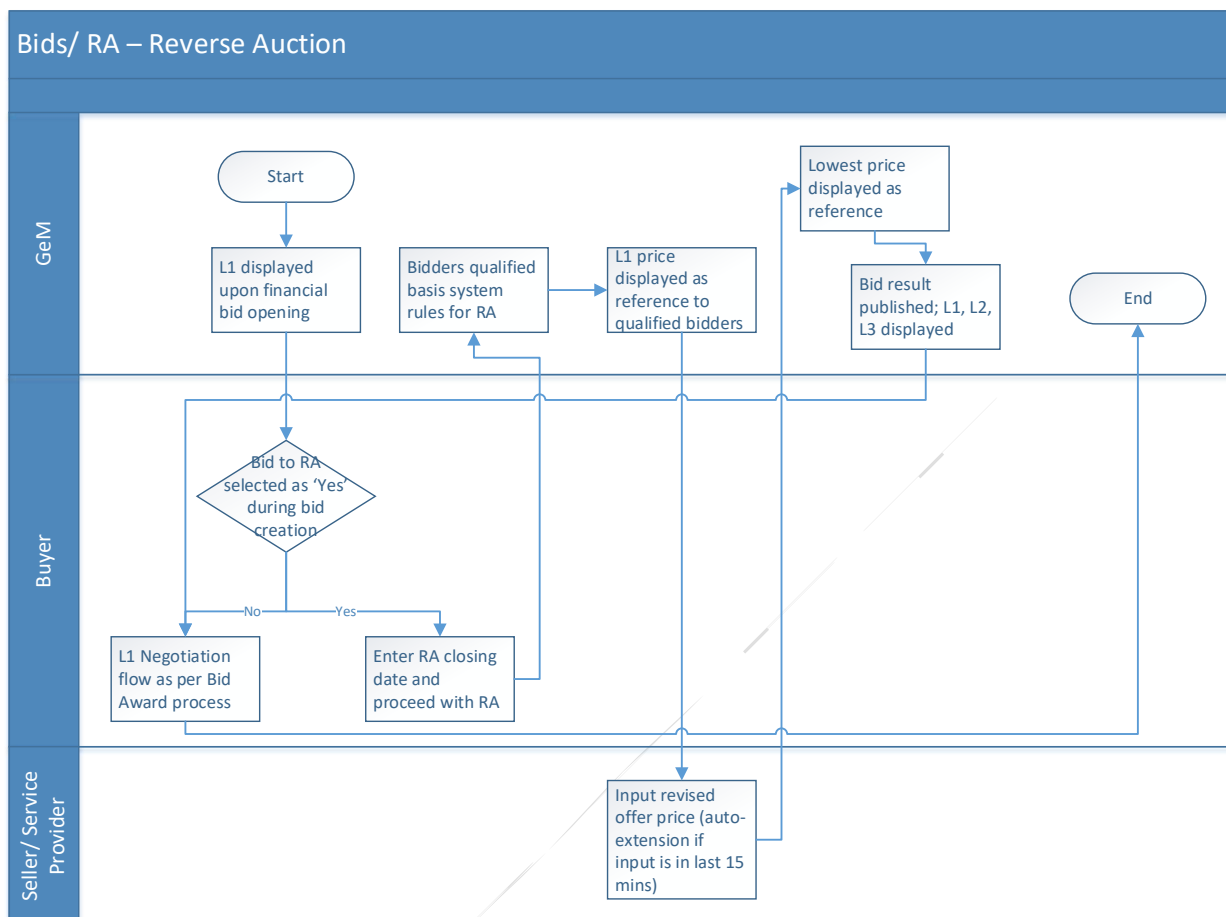
Figure 24: Reverse Auction

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Buyer enters RA related details such as start time, closing date and time, number of rounds, etc.	1.1	Functionality to define number of auto-extensions (can be unlimited as well) during RA creation. Minimum 24 hours extension allowed
2	Eligible bidders are selected and L1 price displayed as reference to qualified bidders	2.1	GeM assesses bidder eligibility for RA and notifies qualified bidders via email and SMS

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
		2.2	L1 price reference displayed to qualified bidders In case of Direct RA, estimated bid price referenced as L1 price to compete
		2.3	In Direct RA, all technically qualified bidders moved to RA
3	Qualified bidders input revised offer price	3.1	Auto-extension of RA if input is in last 15 mins
		3.2	Lowest price is displayed for bidders as a reference
4	Once the bidders have submitted their inputs, bid results are published and L1, L2, L3 Sellers/ Service Providers are displayed	4.1	Assessment of input offer price to display L1, L2, L3 Sellers/ Service Providers with masked names

Table 47: Reverse Auction process & functionalities

Direct Reverse Auction (RA) – Evaluation and Award

Direct RA Evaluation process is similar to the Bid Evaluation process described above. It consists of both technical and financial evaluations. The detailed process has been highlighted below in the process flow:

Figure 25: Direct Reverse Auction Evaluation and Award process & functionalities

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Buyer logins, open the relevant published RA and opens the technical RA for all participating Sellers / Service Providers and assesses the technical specifications submitted (e.g., document verification, criteria met or not and other details review)	1.1	Functionality for Buyers to accept and reject technical specifications and add relevant comments/ select reason for rejection from dropdown list
2	If needed, Buyer can seek clarifications, additional information / documents from participating Sellers/ Service Providers within defined timelines	2.1	Rule based bid freezing until defined timelines for participating Sellers / Service Providers to respond to clarifications

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	Buyer completes technical evaluation and qualifies or disqualifies respective participating Sellers / Service Providers on the basis of pre-defined criteria in the bid	2.1	Automated notifications to technically qualified Sellers / Service Providers
3	Any participating Seller / Service Provider has the option to raise a disqualification challenge till 48 hours of the evaluation completion and Buyer needs to address the same within pre-defined timelines prior to opening the financial bid Post challenges time is completed, financial bids are opened in the system and system automatically displays the lowest cost or price bid (L1)	3.1	Rule based bid freezing until defined timelines for Buyers to respond to disqualification challenge raised
		3.2	Automatic assessment and display of L1 price with Seller/ Service Provider name masked
4	Buyer creates demand and generates purchase order. Buyer also has the option to cancel RA or seek offer validity extension with L1 Seller/ Service Provider's mutual consent	4.1	Notification to selected Seller(s)/ Service Provider(s)

Table 48: Reverse Auction process & functionalities

8.1.6.4   Bill of Quantity (BoQ)

BOQ-based bidding was introduced to enable Buyers to analyze item-wise price breakup in a larger contract/project and purchase varying quantities of multiple items from one or multiple Sellers. During Bid creation, Buyers should have an option to upload BoQ(s) (Bill of Quantities) against an item or multiple items. Sellers can then quote prices for each Sub Item in the required BoQ format (GeM system will auto calculate the total price from each BoQ and populate against that item during bid evaluation).

While other process steps are similar to a Bid/RA process as explained above, BoQ based bidding process differs from a typical bid due to differences in the following two processes:

1. BoQ bid creation
2. Seller participation

Both these processes are described in detail below.

BoQ bid evaluation also differs from a typical bid evaluation as the Buyer has three evaluation options available during the BOQ bid creation process:

1. Total Value wise evaluation: Evaluation basis total value of the bid, awarded to one Seller (L1)

2. Item wise evaluation: Evaluation of each item individually, can be awarded to multiple Sellers (L1) across each item

3. Group wise evaluation: Evaluation of each schedule individually (may include one or more items as grouped by the Buyer)

BoQ based Bid Creation
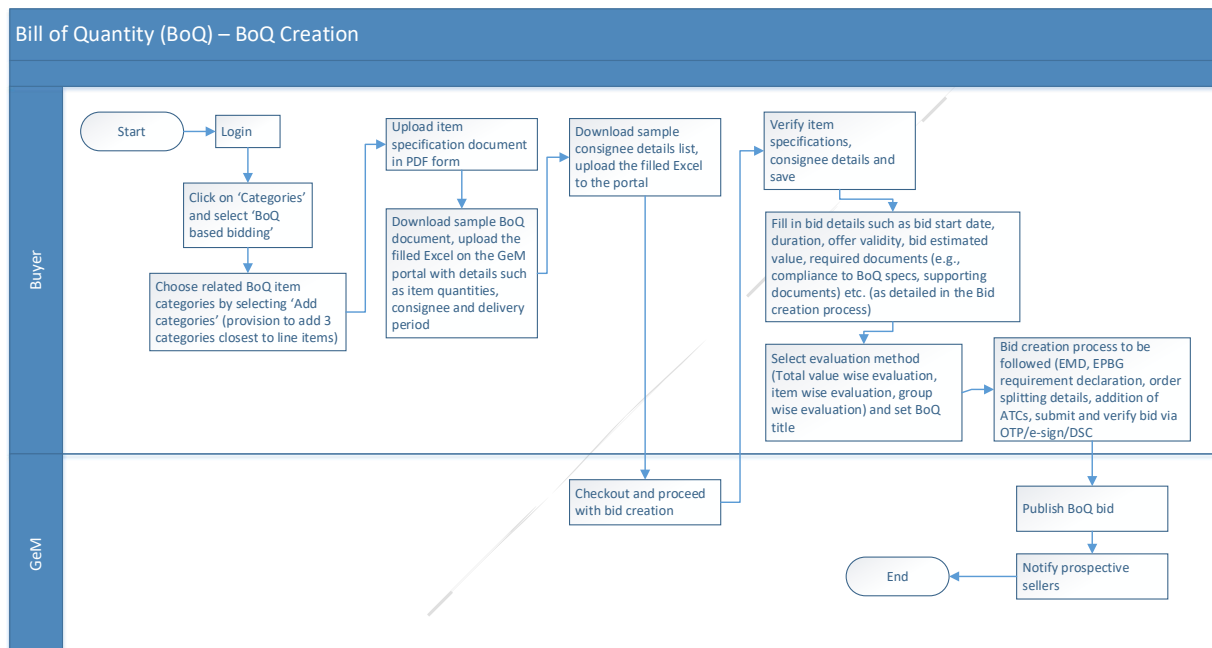
Figure 26: BoQ bid creation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Login, click on BoQ based bidding, choose related BoQ item categories by selecting 'Add categories' (provision to add 3 categories closest to line items)	1.1	Category search and selection

Detailed Process Flows			
#	Process Steps	#	System Functionality
2	Upload item specification document in PDF form. Download sample BoQ document and consignee details list, upload the filled Excel on the GeM portal with details such as item quantities, consignee and delivery period	2.1	BoQ document and consignee details document template available on GeM portal
		2.2	Encrypt and store data on cloud
3	Checkout and proceed with bid creation. Verify and save item specifications and consignee details.		
4	Fill in bid details such as bid start date, duration, offer validity, bid estimated value, required documents (e.g., compliance to BoQ specs, supporting documents) etc. (as detailed in the Bid creation process)	4.1	Information on key parameters such as bid opening date, etc. stored and used to implement system-triggered guardrails. For e.g., bid not allowed to be open prior to set open date
5	Select evaluation method (Total value wise evaluation, item wise evaluation, group wise evaluation) and set BoQ title	5.1	Different evaluation dashboards visible to Buyers based on option selected
		5.2	Searchable bid basis BoQ title
6	Standard bid creation process to be followed post this (process described above)		

Table 49: BoQ bid creation process & functionalities

Buyer has to specify the Bid estimate value for all type of Bid evaluation mode. In case of Item wise evaluation, Buyer have to specify the Bid estimate value for every schedule and for Group- Wise Evaluation, the Bid estimated value for each group needs to be updated.

Buyer may specify the BOQ Title so that it could be easily searched after bid is published.

BoQ – Seller Participation
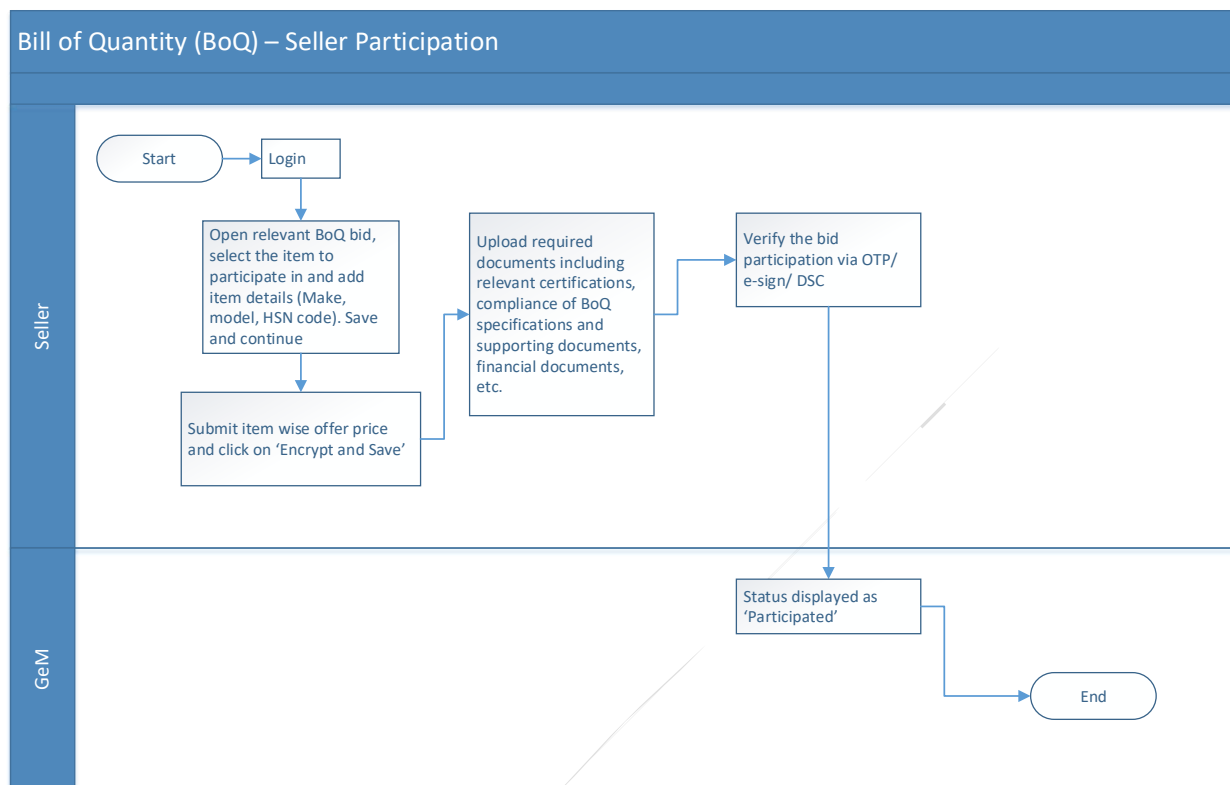
Figure 27: BoQ Seller participation

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Seller opens relevant BoQ bid and selects the item to participate in, adds item details (Make, model, HSN code) and clicks on save and continue		
2	Seller then submits item wise offer price for items selected and clicks on 'Encrypt and Save'	2.1	Encrypted data stored on cloud
3	Upload required documents including relevant certifications, compliance of BoQ	3.1	Store all documents on cloud and make available to Buyer for review

Detailed Process Flows			
#	Process Steps	#	System Functionality
	specifications and supporting documents, financial documents, etc.		
4	Verify the bid participation via OTP/ e-sign/ DSC Status displayed as 'Participated'	4.1	Functionality to enable digital signature / e-Sign based authentication
		4.2	Trigger OTP for verification to Buyer & verify using the input

<p align="center">**Table 50: BoQ Seller participation process & functionalities**</p>

8.1.6.5   Custom Bid

Many times, Buyers have requirements to define bids for categories which are not part of the current GeM category set. Creating a GeM category definition may take time due to the due diligence process involved. Therefore, Custom Bid functionality has been introduced for Buyers to enable creation of custom catalogue-based bid for items not available on GeM. Buyers has to generate a GeM availability report which will indicate whether the desired product/ service is available on GeM or no. Buyer will be allowed to create one bid against each GeM Availability Report generated. Buyer can then define custom catalogue-based bid depending on their needs. The Sellers/ Service Providers would participate in the bid based on the requirements defined by the Buyer and would be required to create a custom offering for the same and offer the same in the bid. The competent authority approval is also required for floating custom catalogue bid.

Custom bid functionality allows:

1. Buyers to create a custom catalogue by providing relevant information such as Title, reference price, selling unit, specifications, drawing documents, reference images, related categories etc. for unavailable items post creation of GeM Availability Report (GAR)

2. Buyers to bunch 2 or more custom catalogue

3. Sellers to participate and confirm compliance to the Buyer custom catalogue requirement. The Sellers will be required to create a custom offering for the same and offer the same in the bid

4. The custom catalogue requirements will be part of the order and the contract

This functionality can be used for the following:

1. Procurement of specialized products that are currently not available on GeM

2. Procurement of technical/engineered products that would require detailed specifications, drawings etc. Feature of uploading custom specifications & drawing documents has been provided.

3. Procurement of additional/side products that the Buyer wants to procure but are not available on GeM

4. Procurement of any one-time service/ bunch of services such as site survey, one-time audit service, one-time training etc.
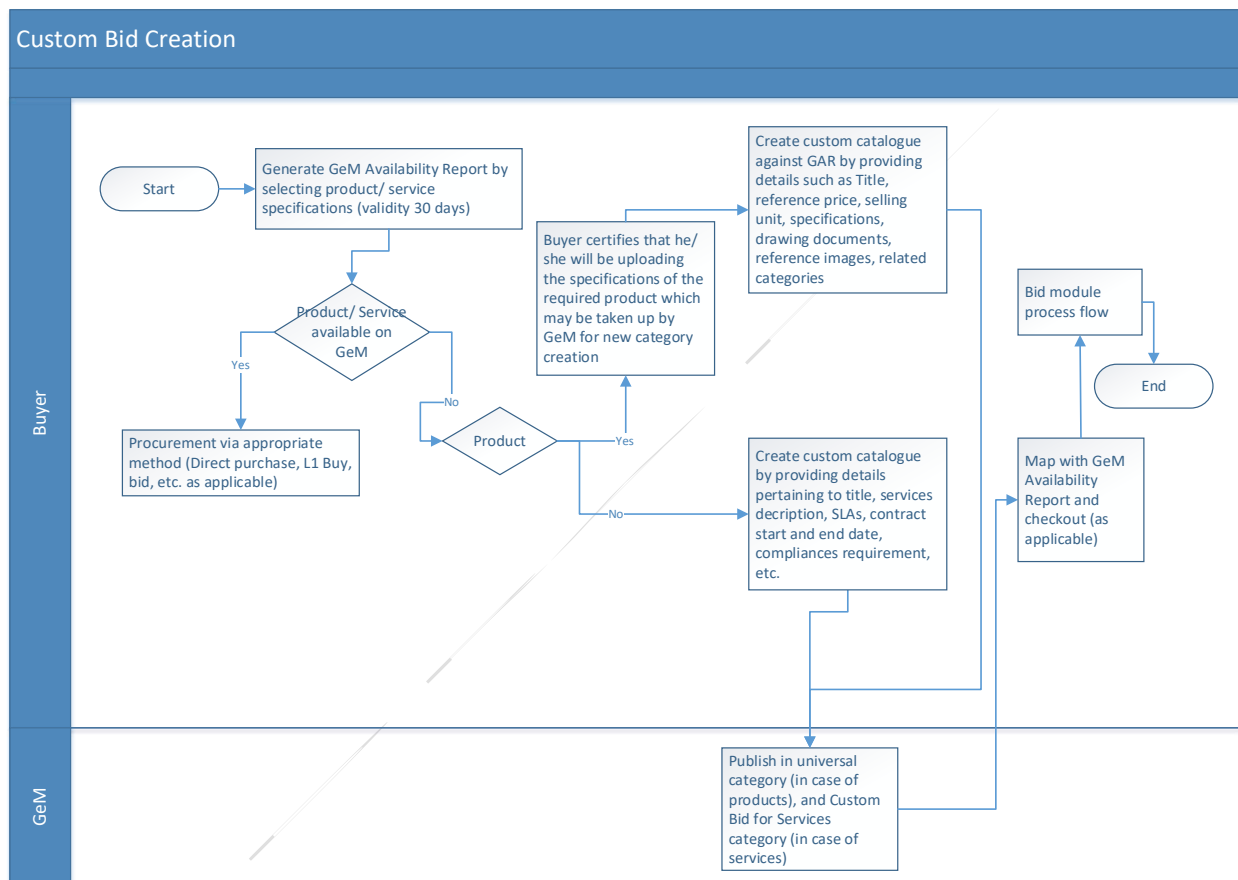
Figure 28: Custom bid creation
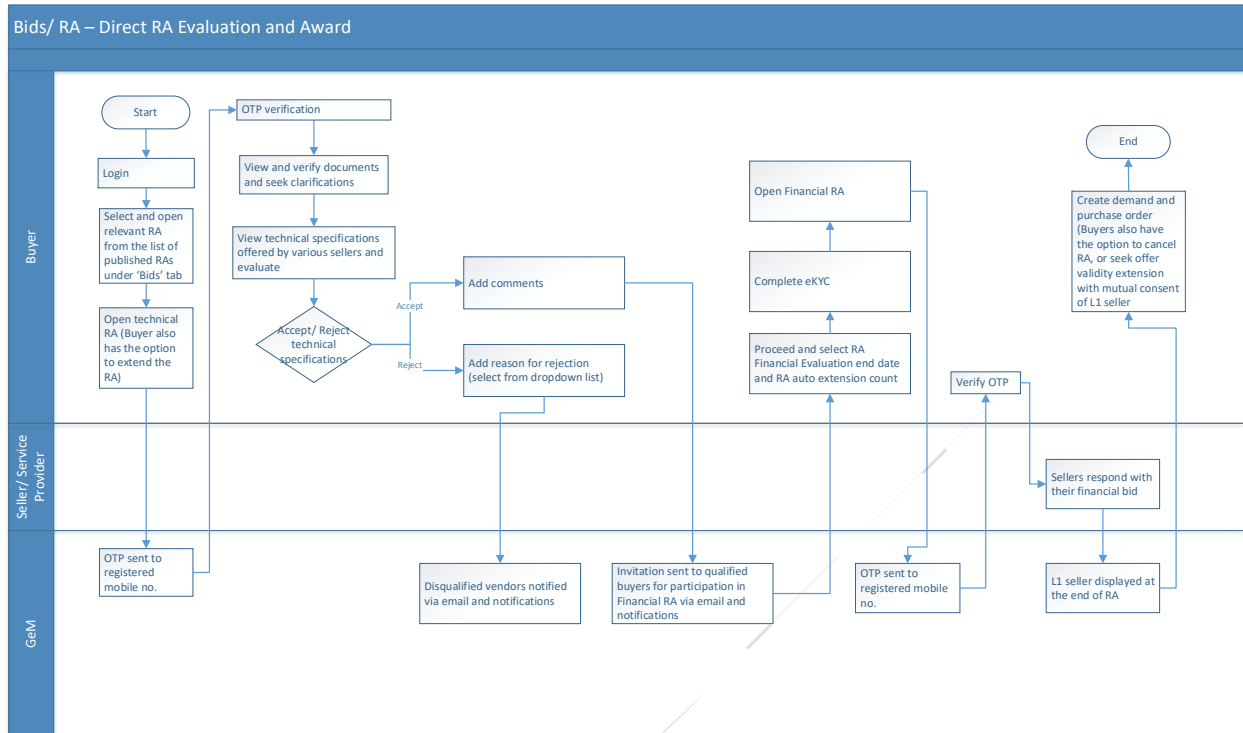
Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyer generates the GeM Availability Report (indicates availability status of products or/and services searched on GeM and past transaction history for the matching product categories. by selecting product/ service specifications	1.1	Generation of templatized availability report with unique ID and past transaction history basis product/ service specifications provided by Buyer
2	If the product/ service is available on GeM them Buyer procures it using suitable method		
3	In case the desired product/ service is not available on GeM, Buyer can purchase the same via custom bid from outside of GeM. Buyer can create only one bid against one GeM Availability Report (GAR)	3.1	Rule-engine to ensure only one bid can be generated against one GeM Availability Report
4	To create a bid, Buyer creates a custom catalogue by providing details such as	4.1	Catalogue creation basis input parameters and publishing within universal category
	1. Product specification undertaking, Title, reference price, selling unit, specifications, drawing documents, reference images, related categories in case of product	4.2	Documents upload functionality and storage on cloud
	2. Title, services description, SLAs, contract start and end date, compliance requirements in case of services	4.3	Functionality to edit pending catalogues
	Unpublished/ pending catalogues can be edited and published anytime		
	Buyer can use an existing custom catalogue, created previously, to create future bids against new GARs		
5	Map custom catalogue with GeM Availability Report via Choose GAR and proceed to	5.1	Option to map existing catalogues to new GARs

Detailed Process Flows

#	Process Steps	#	System Functionality
	checkout, post this the typical process for bid creation is followed	5.2	Custom catalogue with GeM Availability Reports mapping

Table 51: Custom bid process and functionalities
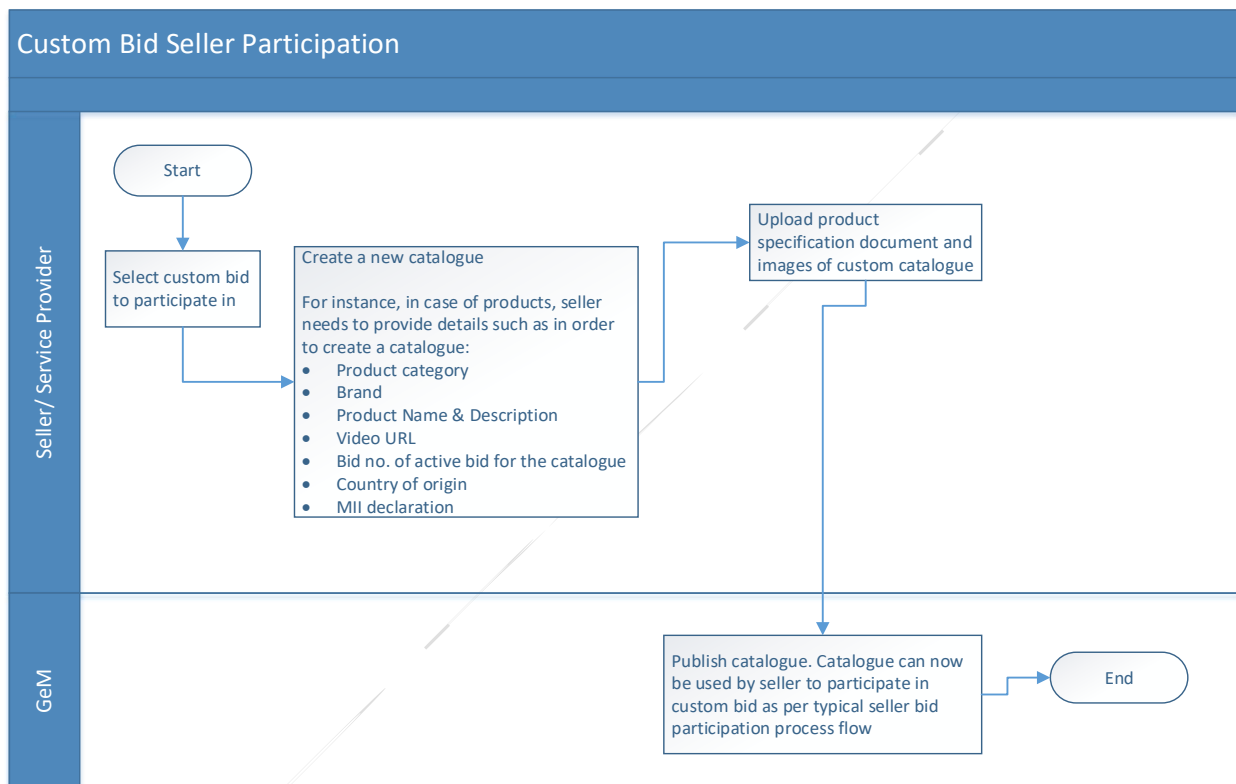
Figure 29: Custom bid Seller participation

Detailed Process Flows

#	Process Steps	#	System Functionality
1	Select custom bid to participate in	1.1	All custom bids that the Seller/ Service Provider is eligible for visible on Seller dashboard
2	Create a new catalogue by providing following details: 1. A similar product or service category 2. Product name & description, video URL, bid no., country of origin, etc. as applicable for products 3. Type of services, no. of people needed, service duration, SLAs, etc. as applicable for services	2.1	Catalogue creation basis input parameters and publishing within appropriate categories for products and services
3	Seller/ Service Provider uploads product/ service specifications document and creates the catalogue. The catalogue then gets published in appropriate category for product/ service.	3.1	Document upload functionality and storage on cloud
4	Catalogue can now be used by Seller to participate in custom bid as per typical Seller bid participation process flow		

Table 52: Custom bid process and functionalities

8.1.6.6 Demand Aggregation

Demand Aggregation was introduced on GeM to help central ministries/ states aggregate the demand for products across departments or organizations in order to drive better price discovery and economies of scale. It will help the buying organization to raise the demand indent for aggregation of the goods at various levels as part of the price discovery process and therefore facilitate procurement of aggregated goods through bid only. All the buying organizations who wish to participate will raise an indent and aggregated demands will take the form of bid. The demand can have various delivery milestones as well as linked to payment so that the price discovered in the process will allow the buying organization to create orders for processing and execution of the goods.

The Seller will have the facility to offer the prices for the goods as per the process of the current Bid system so that large quantity procurement will benefit the Buyer organization.

A demand aggregation request for a specific product can be created by a DA Buyer (secondary user identified assigned the role of DA Buyer in the system). Non-DA Buyers (all other secondary users linked to the concerned central ministry/ state) can then submit their indents by providing details such as the quantity of product, consignee details, etc. Post this, DA Buyer approves/ rejects indents and accordingly creates a consolidated bid. Bid creation, Seller participation and evaluation processes are the same as described above in the Bids/ Reverse Auction section. Once the evaluation is complete and L1 is identified by the system, DA Buyer can view the Demand Aggregation Breakup and select the Sellers and create the master order. Following this, non-DA Buyers can generate the contract and place the individual orders successfully.
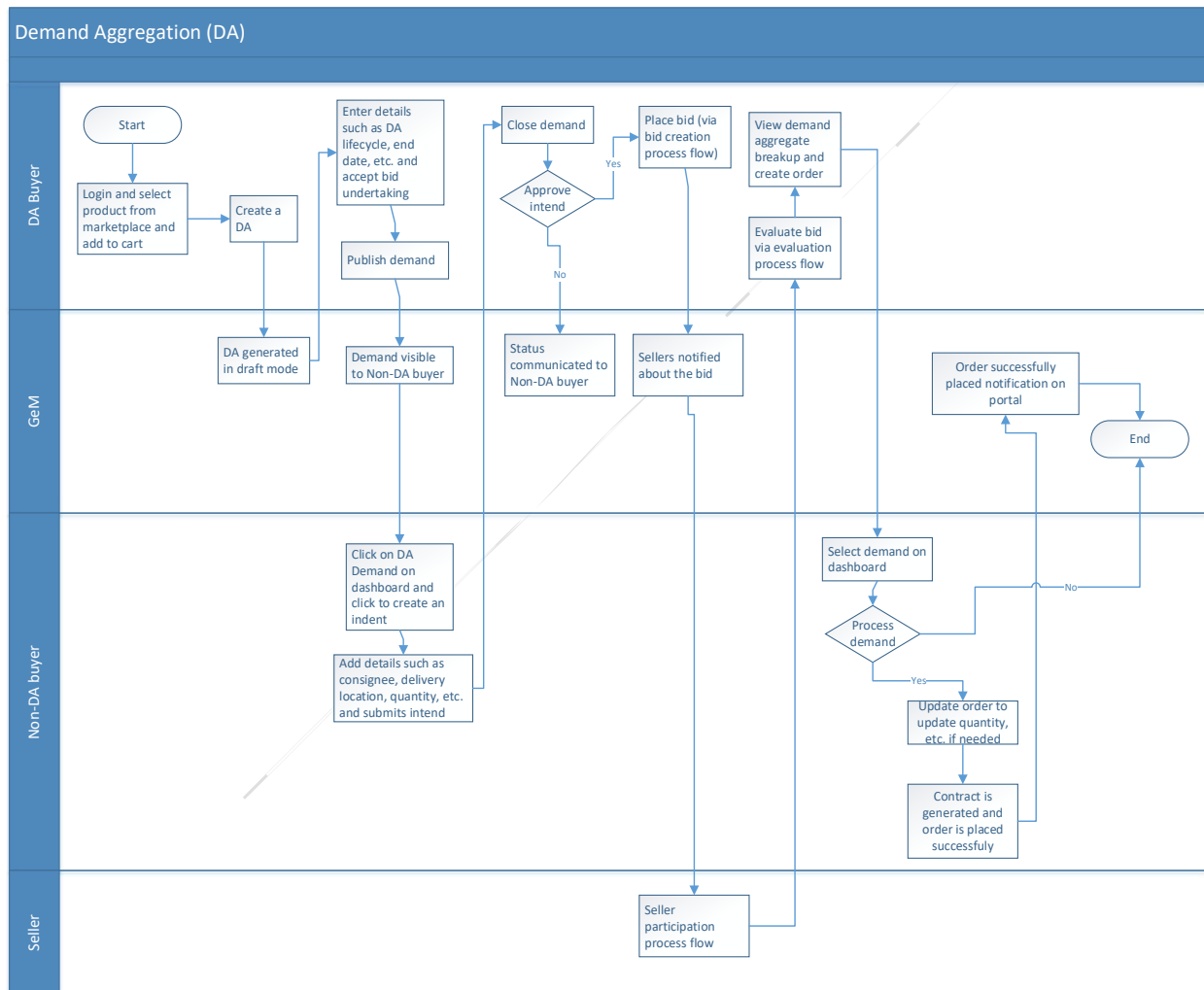
Figure 30: Demand aggregation

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	DA Buyer selects any product from the market and adds item in Cart to create DA Demand. Demand generated in draft mode. DA Buyer enters details such as DA lifecycle, end date, etc.	1.1	Secondary Buyer assigned the role of DA Buyer from back-end
2	DA Buyer accepts bid undertaking if multiple items are in a cart and publish demand	2.1	Demand creation, DA no. generation and DA status updated as published
3	Non-DA Buyer clicks on 'DA Demand' on Dashboard and clicks to create Indent	3.1	DA visible to all Buyers mapped to a particular ministry/ state
4	Non-DA Buyer can now add consignee details such as state, delivery location and quantity and submits intend	4.1	Data stored on cloud
5	DA Buyer closes demand so any non-DA Buyer cannot participate	5.1	DA closed as per end date mentioned, or prior to end date when DA Buyer clicks close demand option
6	DA Buyer clicks on 'Process' to approve or reject intends. Approve intend and click 'Place bid' option to create bid	6.1	In case of rejection, status is communicated to non-DA Buyer on GeM portal
7	Follow bid creation process to create bid with option to define staggered delivery plan		
8	Post this, Sellers are notified about the bid and participate as per the standard Seller participation		
9	Post bid participation, DA Buyer evaluates and awards the bid. Bid is evaluated as per standard process flow. Post L1 display, DA Buyer can view Demand Aggregate Breakup and click on create order option. Post this, the page redirect to the Demand Aggregation Details	9.1	Demand aggregate breakup generated basis submitted intends
10	Non-DA Buyer creates contract. To do so, he/ she goes to dashboard and clicks all	10.1	Auto - contract generation basis input details

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	demands. He/ she then chooses to process/ decline demand or request offer validity extension. Non-DA Buyer processes demand, then clicks on update order to update quantity, etc. if needed. Following this, contract is then generated, and order is placed successfully	10.2	Order successfully placed notification

Table 53: Demand aggregation process and functionalities

8.1.6.7   Forward Auction

Forward auction functionality enables government entities to sell their items to many potential Buyers. Items are commonly placed at an online auction site. Buyers can continuously bid for the items they are interested in. Eventually the highest bidder wins the item.

The secondary user registered as Buyer on GeM will have to be auto registered as an auctioneer onto the Forward Auction (FA) Module. To access the forward auction module, Auctioneer will need to first log-in onto the GeM Portal using their User ID and Password. Post successful log-in, the Buyer will be able to access the FA module. The link will redirect (SSO Login) the Auctioneer to the FA Dashboard where she/he would be able to create their category, create auctions, configure auction parameters (such as start price, increments, time-extension etc.).

The Buyers/ bidders will have to register themselves separately, to access the Forward Auction module and participate in the auctions.

Currently GeM allows for both open and limited forward auctions to be hosted on the platform.

Forward Auction consists of three major aspects, that are explained in detail below:

1. Forward Auction creation and monitoring

2. Bidder registration and participation

3. Forward Auction award

Forward Auction Creation & Monitoring
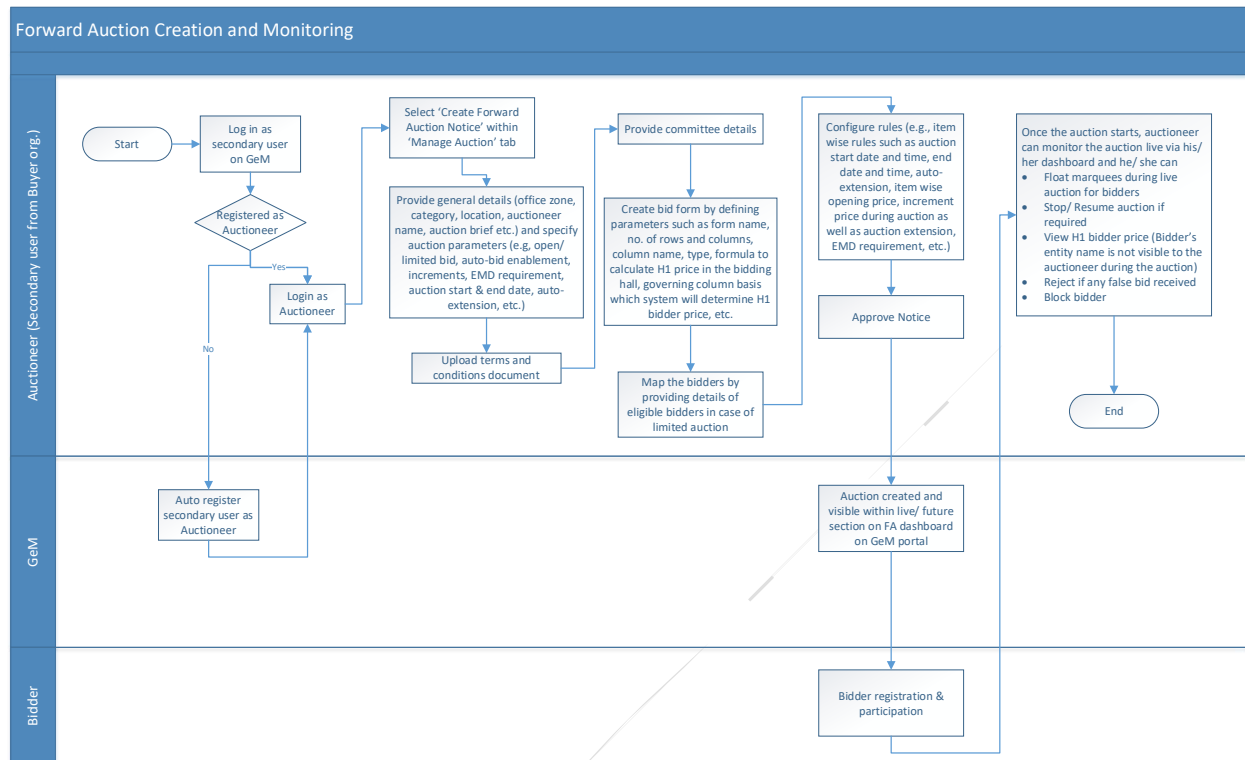
Figure 31: Forward Auction Creation & Monitoring

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Secondary user from Buyer organization logs in to GeM portal and clicks on Forward Auction tab. In case he/ she is not registered as an auctioneer, he/ she will be auto registered. If the secondary user is already registered, he/ she logs in as an auctioneer. (Once registered, he/she can login directly into the Forward Auction module as well)	1.1	Auto registering for forward auction for secondary Buyer users already registered on GeM portal
2	To create a forward auction, the auctioneer clicks on 'Manage Auction' tab. Here the	2.1	Auction dashboard for auctioneer providing details around pending, live,

#	Process Steps	#	System Functionality
	auctioneer can view all the auctions that he has live, pending, future auctions, etc. The auctioneer then selects 'Create Forward Auction Notice'		future, cancelled, and closed auctions. Auctioneer can also download event notice once created, documents, view auction results, etc.
		2.2	Search functionality for auctions
3	To create a forward auction notice, the auctioneer needs to provide some general details such as office zone, category (e-waste, land or buildings, machinery, scrap), auctioneer name and details, project location, reference no., etc. Apart from these details, the auctioneer needs to define basic auction rules as well. For example, bid submission rules (open/ limited), increment in multiples (Applicable/ Not applicable), auto-bid (Applicable/ Not applicable), requirement of EMD/ e-PBG, item wise auction time, auto-extensions, payment start & end date, etc. Post this the auctioneer uploads the general terms & conditions document	3.1	Details & documents stored on cloud
		3.2	Document upload functionality
4	Auctioneer then provides the details of the committee as per discretion of Buyer org.		
5	After this a bid form needs to be created by the auctioneer that will define what fields to be captured in the auction and how to calculate the H1 bidder price. Auctioneer defines parameters such as form name, header, footer, no. of columns, no. of rows. He/she then configures column headers (e.g., Plot details, location, area in sqmt, quantity, rate per sqmt, etc. for land auctions), column data type, filled by, display/ hide columns, etc. After configuring the bid matrix details, auctioneer selects	5.1	Bid form creator and editor functionality
		5.2	Automated calculations of H1 bid price basis defined formula and governing column

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	relevant field and creates formula to command system to calculate the price in bidding hall (e.g., total rate = area in sqmt X rate per sqmt, etc.) Finally, auctioneer selects the governing column which will be used to determine the H1 bidder price in the auction		
6	Auctioneer provides the details of bidders to be invited for limited auctions		
7	Configure rules: Auctioneer configures the overall and item wise auction rules such as auction start date and time, end date and time, auto-extension, item wise opening price, increment price during auction as well as auction extension, EMD requirement, etc.	7.1	Pre-checks and running of auction basis rules defined by auctioneer
8	Once these details have been finalized, auctioneer clicks on 'Notice & Documents', selects 'Approve' within the Notice row, reviews the auction notice and then clicks on 'Approve'.	8.1	Auto generation of event notice basis details provided
9	The approved auction notice will be live for bidders to participate. They can download the event notice, pay the EMD if required (offline process) and upload the EMD details on the GeM portal. Once the EMD is paid, auctioneer can accept/ reject EMDs from his/ her dashboard. Only the bidders whose EMD has been accepted can participate in the auction.	9.1	Auction shown in the live/ future tabs for bidders on the Forward Auction dashboard. In case of limited auctions, eligible bidders are notified via e-mail and on GeM portal
		9.2	Bidder participation enabled post EMD verification
10	Once the auction starts, auctioneer can monitor the auction live via his/ her dashboard and he/ she can	10.1	Configurable Marquees displayed to bidders mid-auction to provide them relevant information
		10.2	Real-time H1 price update

Detailed Process Flows			
#	Process Steps	#	System Functionality
	1. Float marquees during live auction for bidders 2. Stop/ Resume auction if required 3. View H1 bidder price (Bidder's entity name is not visible to the auctioneer during the auction) 4. Reject if any false bid received 5. Block bidder	10.3	Functionality to block bidder, stop/ resume auction and reject false bids

Table 54: Forward auction creation & monitoring process and functionalities

Bidder Registration and Participation
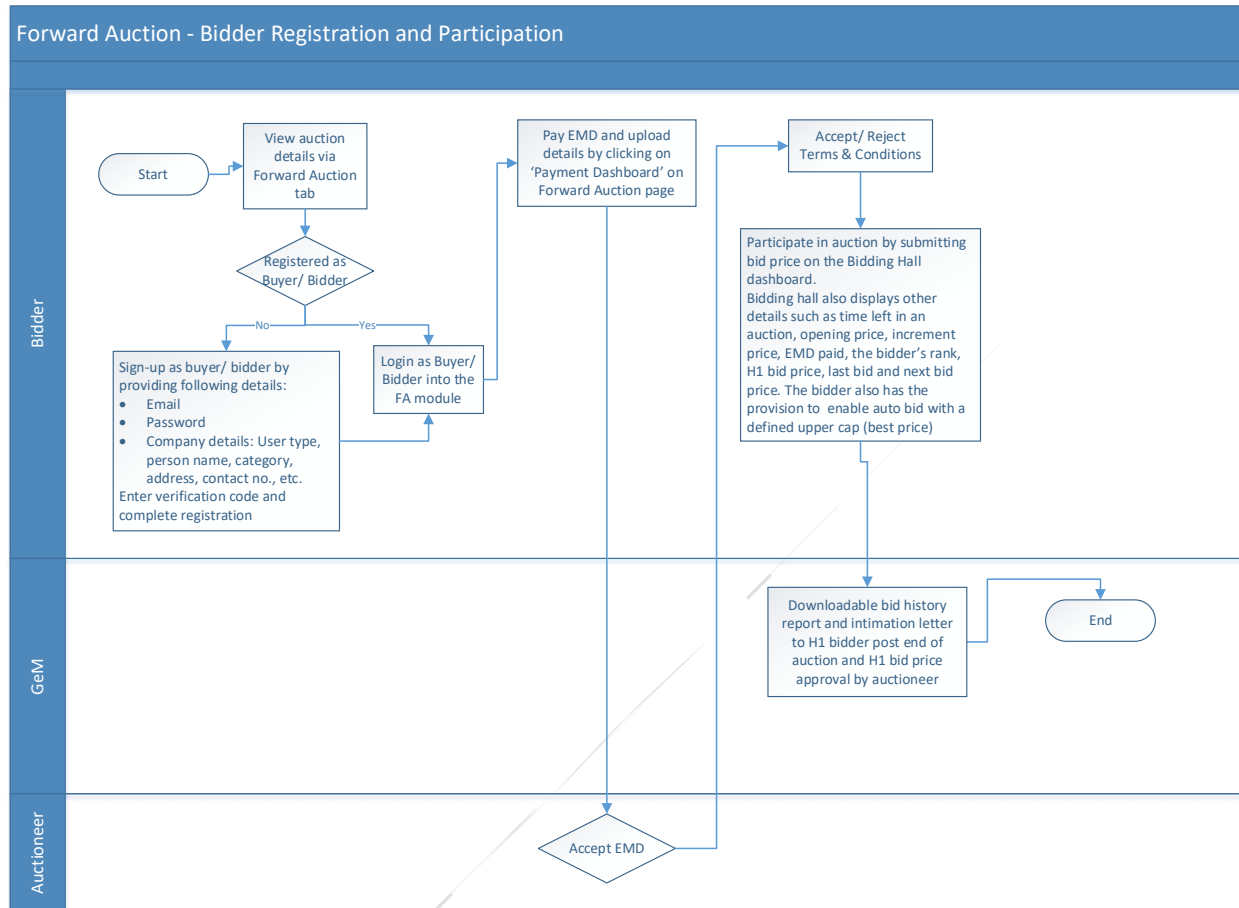
Figure 32: Bidder Registration and Participation

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Potential bidders can view the live/ future auction notices on the Forward Auction dashboard on GeM even if they are not registered. They can view EMD		

#	Process Steps	#	System Functionality
	requirements, business rules and download key documents such as terms and conditions		
2	To participate in an auction, a bidder first has to register himself/ herself on the GeM portal. Bidder clicks on sign-up tab and selects Buyer, post which a Bidder/ Buyer Registration form opens. Bidder provides details such as: 1. Email 2. Password 3. Company details: User type, person name, category, address, contact no., etc. Bidder enters the verification code displayed and completes the registration.	2.1 2.2	Store data on cloud Verification code generation and validation
3	Once registered, bidders can sign-in to the Forward Auction module. The dashboard offers the bidders various options. Bidders can view the live, closed, cancelled, and limited auctions they are invited for. Additionally, they can view the event notice, download relevant documents, update bank guarantee details, and accept terms and conditions	3.1	Auction dashboard for bidders providing details around live, future, and closed auctions. Bidders can also download event notice, upload bank guarantee/ EMD details, view and accept terms & conditions
4	To participate in an auction, bidder first must pay and upload the EMD details on the portal. This can be done by clicking on 'Payment Dashboard' and providing details such as payment mode, reference no., amount, payment date and upload relevant reference documents. This is then submitted to the auctioneer for approval. Auctioneer can accept/ reject the EMD. Only bidders whose EMD has been accepted by the auctioneer would be eligible to place their	4.1	EMD status update post approval from auctioneer

Detailed Process Flows

#	Process Steps	#	System Functionality
	bid in bidding hall. EMD has to be submitted by the bidder within the time period defined by the auctioneer. The status of EMD approval can be viewed on the payment dashboard by the bidder		
5	Once the EMD has been verified, bidder accepts the terms and conditions by clicking on 'I agree'		
6	Once the auction starts, bidder can view and participate in the same from the Bidding Hall dashboard. The dashboard displays reverse clock indicating time left in an auction, opening price, increment price, EMD paid, the bidder's rank, H1 bid price, last bid, next bid price, etc. The bidder also has the provision to view detailed bid history and enable auto bid via the bidding hall dashboard. In case of multiple items, the dashboard has separate section dedicated to each item. Bidder enters the bid amount on the dashboard and submits to confirm the bid.	6.1	Bidding Hall functionality and dashboard to enable live bidding
		6.2	Real-time information on bids from different bidders
7	In case of auto bid, bidder sets the upper cap (auto bid best price), and the system enters and submits the bid basis increments defined automatically till the upper cap has been reached. To resume manual bidding, the bidder can select Manual Bid submission option.	7.1	Auto-bid functionality featuring auto bid submission on behalf of the bidder till a defined upper cap is reached
8	Once the auction ends, the bidder can download the bid history report. In case the bidder turns out to be the H1 bidder and the auctioneer accepts the H1 bid price, an intimation letter is generated and sent to the bidder via email. The bidder can also	8.1	Downloadable reports (e.g., bid history)
		8.2	Auto generation & relaying of intimation letter to H1 bidder post H1 Price acceptance by auctioneer

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
	download the same from the Bidding Hall dashboard as and when required.		

Table 55: Bid Participation process and functionalities

Auction Award:
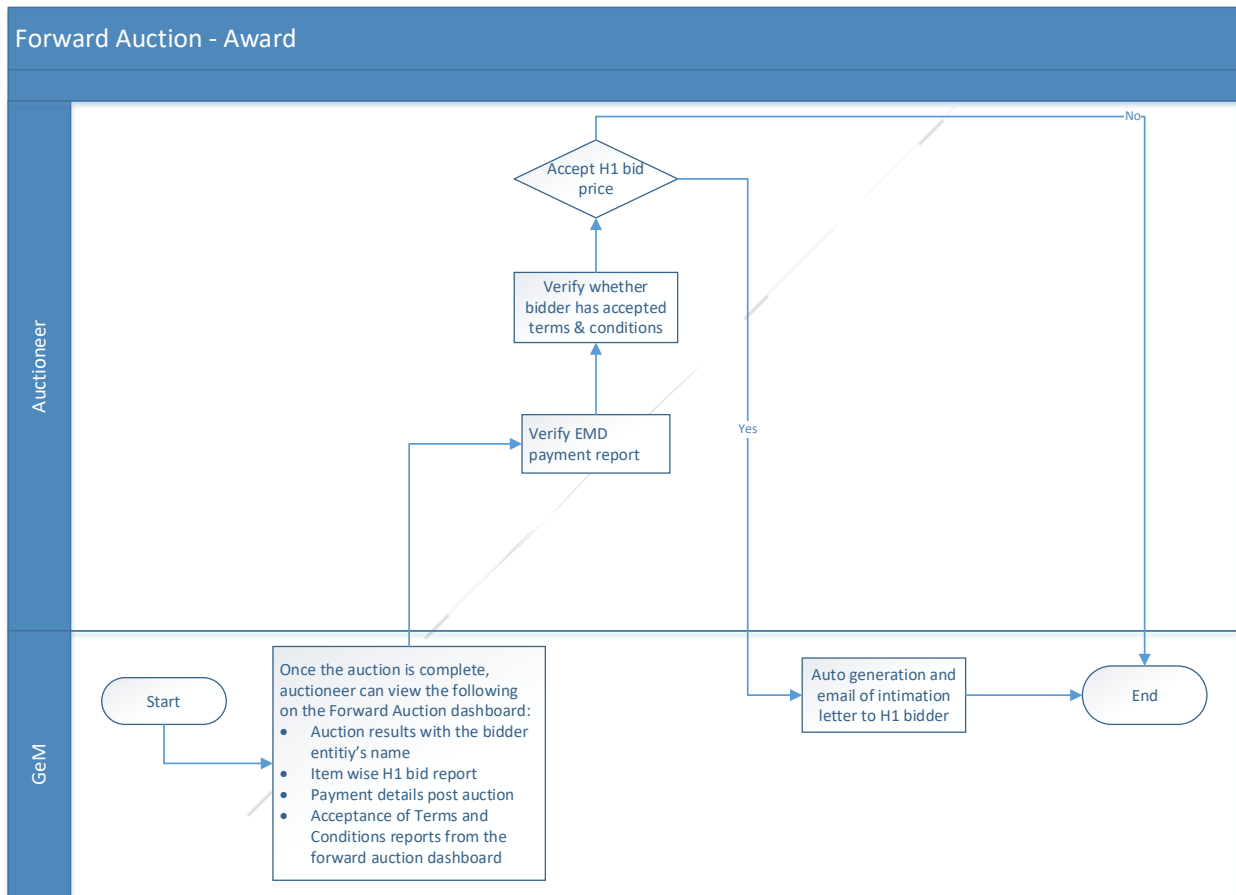
Figure 33: Auction Award

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Once the auction is complete, auctioneer can view the following on the Forward Auction dashboard: 1. Auction results with the bidder entity's name 2. Item wise H1 bid report 3. Payment details post auction 4. Acceptance of Terms and Conditions reports from the forward auction dashboard	1.1	Auto generation of reports
		1.2	Downloadable reports for department perusal – Acceptance of Terms and Conditions report, auction result, Item Wise Leading Bid report
2	Once the auctioneer has verified the EMD payment report, as well as whether the bidder has accepted terms and conditions, he/ she will get a provision to accept / reject of H1 bid price post auction and generate Intimation Letter to H1 Bidder. On acceptance of H1 Bid Price, system will e-mail intimation letter to H1 Bidders	2.1	Auto generation and e-mail of intimation letters post H1 price acceptance
3	Lastly, auctioneer can also view Auction Audit Trail Report, Auction Gain Report, Asset Auction Report, etc. via Forward Auction MIS	3.1	Analytics and auto generation of various, downloadable data reports

Table 56: Auction award process and functionalities

8.1.6.8   Additional interventions/ functionalities required:

Direct Purchase/ L1 Buy:

1. Provision for robust rule based engine to enable customizable purchase limits for all e-procurement archetypes - direct purchase, L1 buying, Bid and RA, etc. across different Buyer organizations e.g., Each state requiring different purchase rules basis state-specific procurement acts

2. Primary Buyer should have provision of configurable budget blocking. So that if any organization wants to block only 50% or even wants to proceed without blocking, they can do for their organization.

3. Historical price trend data to be made available for services as well on the basis of technical specifications selected

4. Enable bunching in market for Services as well

5. Allow addition of multiple consignees in case of Services

6. Filter of verified Seller to be enabled at marketplace

7. Provision for OEM dashboard and PAC (Proprietary Article Certificate) buying for Services (allows buying from a specific entity repeatedly)

8. Predictive prompts and guides to first time users to ensure easy procuring experience

Bids, RA, DA, Custom Bid, BoQ:

1. Enablement of single stage bidding process *(currently ongoing)*

2. Provision to capture base price and GST breakup of product/ services being procured separately during a bid process. Bidder should have the functionality to bid on the basis of base price

3. Functionality to allow Buyers back and forth navigation across steps in bid creation process for quick modifications of bid parameters such as specifications, quantity, etc.

4. Functionality to clone or leverage an existing tender for pre-filling and if required, editing, all required details in a new tender for enabling quick bid creation e.g., for recurring orders

5. E-Briefcase facility to collect relevant documents used on a recurring basis in bids etc., from Sellers/ Service Providers, e.g., MSE certificate, start-up certificate, turnover certification, relevant experience in case of a services related bid *(currently ongoing)*

6. EMD and e-PBG submission and verification to be enabled in an online mode on the GeM platform. Integration with different banks may be required to enable this process

7. Facilitate Buyers in bid/ contract creation by showing them a list of standard SLAs being used across different tenders of similar services or service category

8. In case of bundling of services, enable capturing of specifications and details across all services selected for the purpose of bid

9. In case of AMC services, Buyer to have provision to select services associated with a previously procured product from the order history/ list on GeM portal (e.g., maintenance services for a particular AC can be procured by visiting the order history, selecting the AC ordered previously and selecting the maintenance services for that particular AC)

10. Demand Aggregation and bill of quantity functionality to be enabled for services as well *(currently ongoing).* The process flows of these functionalities as well as Custom Bid may differ from the process flows in case of products

11. Enable front-end registration for DA Buyer by creating a role for DA Buyer. Currently a secondary Buyer is assigned the role of DA Buyer from the back end by enabling certain functionalities

12. Addition of add-on services to be allowed in case of a bid related to services. For example, in a bid for printing services, Buyer should be able to add design services, etc. if needed

13. Enable procurement via rate contracts on GeM portal to facilitate purchases of items at a fixed price per unit for the time specified in the contract *(currently ongoing)*

14. Allow bundling of goods and services to be procured in a single bid

15. Provision for nomination-based bidding to enable procurement from the same Seller/ Service Provider

16. Develop, implement, and maintain e-procurement module for International Competitive Tenders or Global Tenders i.e., tenders involving suppliers of foreign origin or registration and multi-currency transactions

17. Functionality for Buyer to choose invoicing type (cyclic, performance based, milestone based) and correspondingly define milestones, and performance criteria and payment terms, during bid creation, in case of services

18. Functionality for Buyers to upload service details (e.g., no. of months, minimum wages, scope of work, multiple formulae, SLAs, specifications, etc.) via a macro-based Excel or a user-friendly interface

19. Enable upload of details via an Excel sheet in case of BoQ based procurement

20. In case of emergence of multiple L1s within service, Buyer should have the provision to select the L1 manually by giving relevant reason or choose the L1 randomly selected by the System (Run L1). In case Buyer wishes to proceed with the randomly selected L1 by the system, Buyer needs to provide an approval from the competent authority *(currently ongoing)*

21. Service category specific SLA library with provision for consignees to add own SLAs as well. SLAs must be modifiable throughout the duration of the contract. Deductions to be auto-calculated by the system as per the SLAs defined and details (e.g., SLA breached, no. of breaches, etc.) provided by the consignee. Option to be provided to Buyer to terminate the contract in case cumulative deductions reach 10% of the total contract value or more. These limits must be configurable by the GeM team, with proper approval process, via a front-end utility

22. Provision to Buyer to disqualify unworkable L1 after opening the financial bid *(currently ongoing)*

23. Provision for limited tendering and Buyer to invite specific Sellers/ Service Providers to participate in a limited tender

24. Provision for customized Terms & Conditions library for Buyers

25. Functionality for mentioning the delivery period and related deviation & price quoting for Sellers during bid participation

26. Functionality for procurement of refabrication (manufacturing) services

27. Vendor rating shall be included as a parameter in bid process. Buyers can select if they only want to include Sellers/ Service Providers with a certain or higher rating

28. Overall improvement and refinement of Custom Bid and BoQ processes

Forward Auction:

1. Provision to add more categories for forward auction through a front-end utility apart from the four currently defined (e-waste, land or buildings, machinery, scrap)

2. Provision to download bid form in Excel format

3. Identify and finalize reasons pertaining to which auctioneer/ bidders can raise an incident in case of forward auctions. Include these reasons within the Incident Management Policy. Integration of Forward Auction module with Incident Management Module

4. Enable forward auction for services such as parking facilities, etc. For any service procured via Forward Auction, appropriate invoicing and post contract management processes shall be developed and implemented

5. Provision for H1 Bidders to pay the transaction charges online to GeM *(currently ongoing)*

6. Provision for Bidders to pay EMD online *(currently ongoing)*

7. Provision for Bidders to upload TDS certificate on GeM *(currently ongoing)*; TAN Number of Bidders to be captured for TDS purpose

8. Functionality to reimburse additional TDS charges

9. The location of Auction/ Location of Assets shall be captured systemically *(currently ongoing)*

10. Compliance with ITR service and upgradation of PAN API

11. Advanced, NLP enabled, search for Bidders to search by location (user can search auction by state, district and pin code) *(currently ongoing)*

12. Limited Auction Bidding access change: Bidders to be allowed to be added in Forward Auction 24 hours before auction is complete *(currently ongoing)*

13. Configurable time-gap (~4 hours) between Auction stop and resume date and time with push notifications to bidders on auction stop and resume

14. Provision for Auctioneer to provide a platform and clarification window to bidder for asking any queries to Auctioneer

15. Authentication check for Buyers/Bidders with valid Aadhaar to get registered on GeM *(currently ongoing)*

16. Functionality for Auctioneer to issue a corrigendum to bidders in case of any change in Auction terms

17. Provision to check and approve the Pre-qualification document

18. Functionality to provide Competent Authority's approval while creating a limited auction

19. Functionality to enable H1 bidder to generate online invoice

20. Provision for Auctioneers to choose from category-specific standard Bidding templates for auction creation

21. HSN code input field should be provided along with GST %

22. Process enhancements such as auto refresh of live bidding page every 5-10 seconds during auction, configuring a business rule to set maximum increment multiples allowed which will restrict users to increase the current price of auction beyond a limit, etc.

23. There should provision for auctioneer to specify a Reserve Price where auction is allotted to H1 bidder if Bid value is >= to Reserve Price

24. Auctioneer should have the option to close their existing user account

25. Transaction charge in case of forward auction to be collected before the invoice generation

Overall:

1. Enable rate contract functionality

2. Enable push button procurement functionality

3. Online provision for inspecting authorities to submit their inspection certificates/ quality assessment and evaluations on GeM

4. Functionality for primary Buyer user to transfer bid process, cart process, auction process, or any other procurement process from one individual to another in case the person overseeing the process goes on leave of absence, gets transferred elsewhere, etc*. (currently ongoing)*

5. Architecture must allow for pagination and indexing of Seller documents uploaded for participation

6. Rule-based system checks (to verify parameters such as turnover, project experience, etc.) which can be configured by CMS admin via a front-end utility for different categories

7. Platform should support bi-lingual (English & Hindi) search capability

8.1.7 Contract Management

Contract Management involves two crucial aspects:

1. **e-Contracting**: e-Contracting makes it easy for Buyers and Sellers/ Service Providers to finalize the terms & conditions and other key aspects of an order placed on GeM. This functionality allows Buyers to create, generate and digitally sign an order/ service contract. GeM system has pre-designed template of contract for each product category. The digitally signed contract is then sent to the Seller/ Service Provider for acceptance. The contract is auto accepted except in cases highlighted in Volume 1 Section 8.1 of this RFP.

2. **Post-contract Management**: This process involves amendments that can be request by Buyer/ Seller/ Service Provider post a contract has been signed by both parties. These currently include quantity amendment and delivery period amendment for products and quantity, contract period amendments and contract extension for services.

The sections below detail out each of these processes.

8.1.7.1 e-Contracting
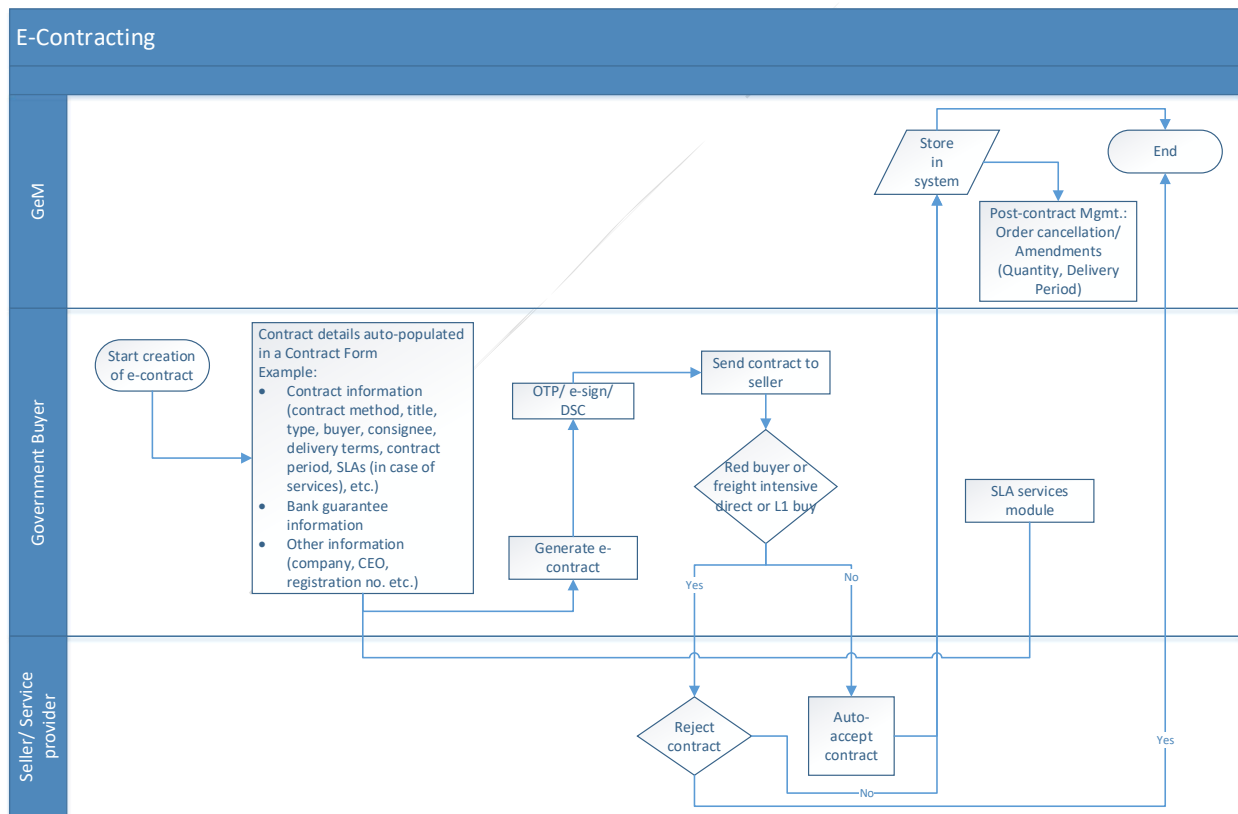
Figure 34: e-Contracting Process

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**

1	Required contract details, such as below, are auto populated in an online form
	
	   1. Contract method
	   2. Contract title
	   3. Buyer and consignee details
	   4. Contract period / Delivery date
	   5. Delivery terms
	   6. SLAs
	   7. Product Details
	   8. Company information
		1.1	Pre-defined, standard contract template

		1.2	Auto-capture of data from bid/ L1/ direct purchase module, etc. to the contract module
2	Buyer generates e-contract and validate it via OTP verification, e-sign or digital signature certificate	2.1	System generates e-contract in predefined template
		2.2	Functionality to enable digital signature / e-Sign based authentication
		2.3	Trigger OTP for verification to Buyer & verify using the input
4	E-contract is auto-shared with Seller/ Service Provider. It is also shared to various ERP systems integrated with GeM portal. In case of direct and L1 purchase, if the Buyer falls within the 'red Buyer' category or the purchase involves freight intensive category (automobile), Seller/ Service Provider gets the option to reject contract. In all other cases, the contract is auto accepted by the system, and stored in the system	4.1	System triggered sharing of e-contract with Seller/ Service Provider post Buyer signature
		4.2	System triggered auto-acceptance or Seller triggered rejection of contract based on defined rules
		4.3	E-contract details stored by the system on cloud
5	Once the contract is stored in the system, Buyer and Seller/ Service Provider have the functionality to amend certain aspects of the contract such as quantity and delivery period or cancel it		

Table 57: e-Contracting process & functionalities

8.1.7.2 Post-Contract Management

8.1.7.2.1 Products

Once a contract has been accepted by the Seller, Buyer and Seller have the functionality to:

1. Amend contract Quantity (Quantity amendment)

2. Amend delivery period agreed in the contract previously (Delivery Period Amendment)

3. Cancel the order/ contract (Order Cancellation)

4. Price amendment in case Price Variation Clause in included in contract

The three functionalities have been explained in detailed below.

Quantity Amendment: This option is only available to the Buyer. Buyers are allowed to increase the quantity by up to 25% (50% in case of Ministry of Defense).

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Buyer can adjust the order quantity by clicking on the 'Quantity Amendment' option against a particular active order on the order summary page.	1.1	Option enabled for active orders
2	Once the Buyer enters the additional quantity required, a separate order is created in the system which is then mapped to the parent order	2.1	Mapping of new order with parent order

Table 58: Quantity amendment process & functionalities

Delivery Period Amendment: This option is available to both Buyers and Sellers. Buyer/ Seller can amend the delivery period (DP) in two ways: DP refixation and DP amendment with Liquidated Damages

1. Delivery Period refixation: In this case Buyer clicks on the DP refixation option provided against a particular active order on the order summary page. Buyer then enters the extension date, and an amendment request is generated, verified by the Buyer via OTP, DSC or e-sign.

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyer clicks on the DP refixation option provided against a particular active order on the order summary page	1.1	Option enabled for active orders with some quantity pending for invoicing
2	Buyer then enters the extension date, and an amendment request is generated, verified by the Buyer via OTP, DSC or e-sign, and sent to Seller/ Service Provider	2.1	Functionality to enable digital signature / e-Sign based authentication
		2.2	Trigger OTP for verification to Buyer & verify using the input
		2.3	Automated sharing with Seller on the portal and email
3	Seller follows the same process to request a DP amendment. But in this case, Buyer has the option to accept/ reject the DP extension request raised by Seller	3.1	Acceptance/ rejection of DP amendment request raised by Seller basis Buyer input

Table 59: Delivery period refixation process & functionalities

2. Delivery Period amendment with Liquidated Damages: In this case the Seller is liable for Liquidated Damages in accordance with the delay in delivery. Buyer/ Seller follows the same steps described above to generate, validate and share the DP amendment request with the other party, who then accepts or rejects the request.

Detailed Process Flows			
#	Process Steps	#	System Functionality
	Steps 1- 2 are same for Delivery Period amendment with Liquidated Damage for both Buyers and Sellers		
3	Once the amendment request has been shared with the other party (Buyer/ Seller),	3.1	Acceptance/ rejection of DP amendment request raised by one party basis the other party's input

Detailed Process Flows	
# Process Steps	# System Functionality
they have the option to accept/ reject the same	

Table 60: Delivery period amendment with Liquidated Damages process & functionalities

Order Cancellation: This option is available only to the Buyer. In case the delivery period is inactive, the Buyer can cancel the order without Seller's consent. In case it the delivery period is active, the Buyer follows the below process

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyer clicks on the 'Cancel Order' option provided against a particular order on the order summary page and inputs details such as reason for cancellation		
2	Buyer then validates the request via OTP verification, e-sign or DSC	2.1	Functionality to enable digital signature / e-Sign based authentication
		2.2	Trigger OTP for verification to Buyer & verify using the input
3	A notification is sent to Seller who then accepts/ rejects the request	3.1	System triggered notification to Seller post cancellation request verification

Table 61: Order Cancellation process & functionalities

8.1.7.2.2   Services

In case of services, once a contract has been accepted by the Service Provider, Buyer and Service Provider have the following functionalities:

1. Quantity amendment (available to both Buyer and Service Provider)

2. Contract amendment (contract period decrease or termination) (available to Buyer)

3. Contract extension (available to Buyer)

The process to raise the three amendment requests is similar to the process described above wherein Buyer enters the new quantity/ contract end date and generates an amendment request by verifying via OTP/ e-sign/ DSC. The Service Provider approves/ rejects the amendment request.

8.1.7.3 Additional interventions/ functionalities required:

e-Contracting:

1. Provide an option to negotiate further with L1 Seller/ Service Provider post bid award.

2. Details around Invoicing type (cyclic, performance based, milestone based), milestones and payment terms, should be captured during bid creation and auto-filled during contract generation.

3. Provision to capture base price of products/ services and breakup of taxes including GST separately in the contract and in the system.

4. Proper management of contract repository with each contract stored chronologically with file name starting with year/ month/ date and then contract ID.

Post-contract management:

4. Front-end functionality to amend all data points in a contract/ bid (e.g., consignee details for an order, delivery date, quantity reduction/ increase, contract prices basis fluctuations in price estimators, contract period, etc.) should be available to front end users (Buyer, Seller, Service Provider).

5. Allow partial cancellation and closure of order post authorization in case complete quantity is not available with the Seller or not needed by the Buyer, and rest has been supplied *(currently ongoing)*.

6. Functionality to enable Sellers/ Service Providers to request for and download Project completion certificate from GeM for contracts awarded via GeM. Project completion related status to be viewable on public domain.

7. Modification of a particular contract shall not generate a completely new contract ID but a sub-set of the original contract ID for easy tracking and monitoring.

8. For any service procured via Forward Auction, appropriate invoicing and post contract management processes shall be developed and implemented.

8.1.8 Order Fulfilment

Once the contract is generated and Seller/ Service Provider has accepted the order on GeM, the Seller/Service Provider is required to process and fulfill the order. GeM plays a role within the entire fulfilment cycle via facilitation of various sub-processes such as:

1. Payment of transaction charges/ Annual Milestone Charges from Seller to GeM

2. Performance Bank Guarantee form submission and verification

3. Invoice generation (invoice shall be GST compliant)

4. Submission of proof of delivery

5. PRC and CRAC generation in case of product and SDAC generation in case of services

6. Supplementary invoice generation in case of rejected quantity during PRC/ CRAC
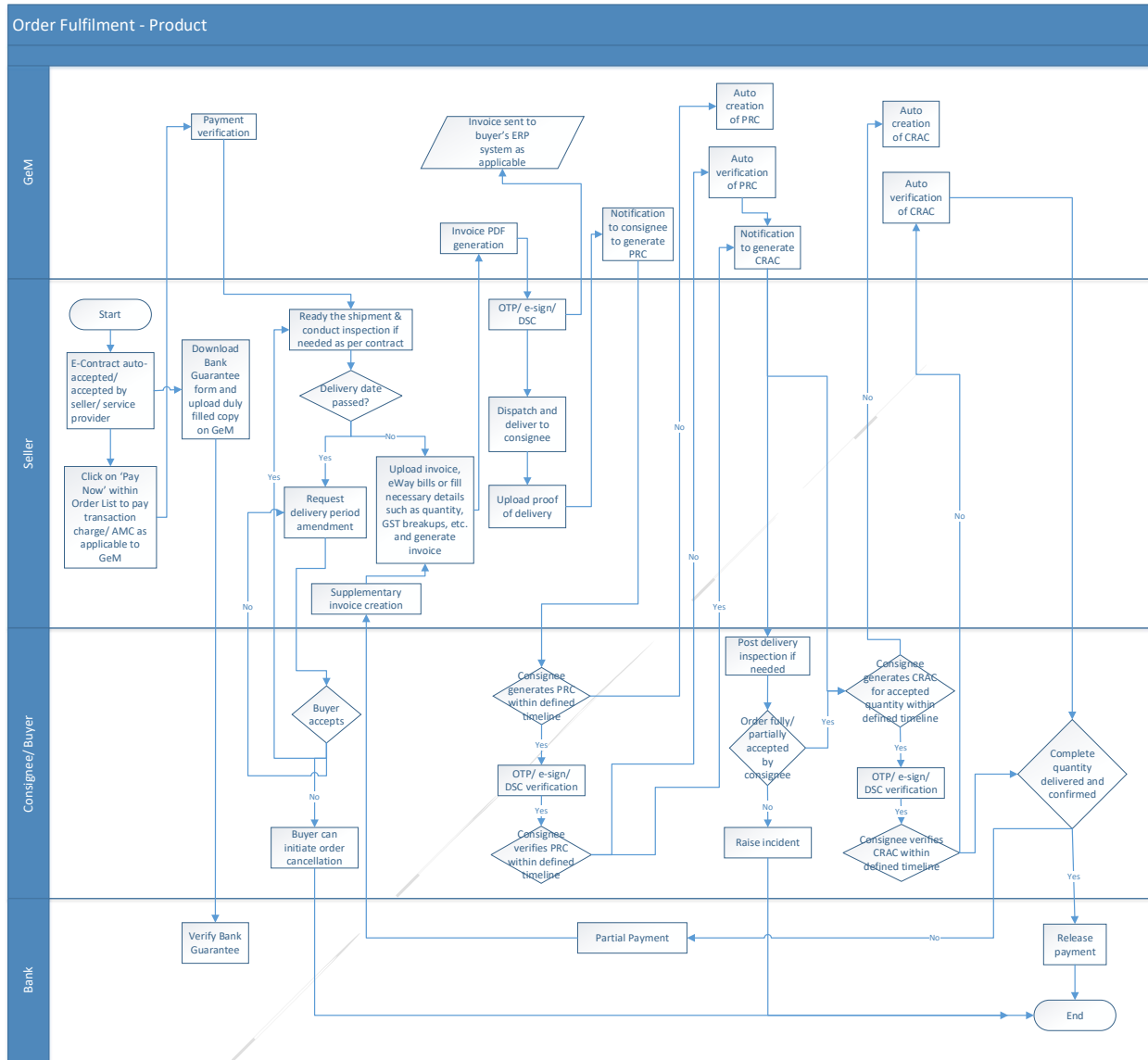
Figure 35: Order Fulfilment – Product

Detailed Process Flows

#	Process Steps	#	System Functionality
1	Seller pays transaction charges/ AMC as applicable post acceptance of contract. Seller can also deduct TDS on accumulative orders of more than a limit.	1.1	Integration with payment modes (e.g., PFMS, IFMS, GPA, Internet Banking, IPAS, etc.)
2	Upon verification of payment, Seller downloads and uploads bank guarantee form on GeM for bank guarantee verification and also sends the hard copy to Buyer	2.1	Store collected documents on cloud
3	Post bank guarantee verification, Seller readies the shipment and conducts an inspection if required as per contract. If the delivery date has not passed, Seller can generate invoice and fulfill the order. Otherwise, Seller needs to request for a delivery period amendment. In case Buyer rejects the request, the	3.1	Deactivate invoice generation functionality basis defined rules
4	Invoice generation via uploading invoices, e-Invoice, eWay bills or filling in necessary information such as quantity, GST breakups, etc. to generate invoice PDF which is then validated by Seller via OTP/ e-sign/ DSC and sent to Buyer's ERP systems wherever applicable	4.1	Generate invoice PDF using input information and documents
		4.2	Functionality to enable digital signature / e-Sign based authentication
		4.3	Trigger OTP for verification to Seller/ Service Provider & verify using the input
		4.4	Integration with ERP systems of select Buyers
5	Once the order is dispatched and delivered to consignee, Seller uploads proof of delivery to GeM	5.1	Store collected documents on cloud
6	Post proof of delivery upload, GeM notifies consignee to generate PRC and once done, CRAC. Once consignee has submitted PRC, he/ she can conduct post-delivery inspection and generate CRAC accordingly	6.1	Trigger notification to consignee at appropriate time period

7	Consignee has to generate and verify PRC and CRAC within defined no. of days (varies by product category) post which the PRC and CRAC is auto-generated and auto-verified by GeM	7.1	Auto-generation and verification of PRC and CRAC basis defined rules
8	In case the complete quantity is delivered & accepted, the payment is released to the Seller. In case some quantity is remaining to be delivered, a partial payment is released by the Buyer post creation of a normal invoice for the quantity delivered. A supplementary invoice is to be created by the Seller against the remaining/ rejected quantity. Additionally, in case the complete/ partial order is rejected by the Buyer, an incident can be raised by either party	8.1	Integration with payment systems such as PFMS, IFMS, GPA, etc. to enable blocking and releasing of payments
		8.2	Incident dashboard to raise and manage incidents

Table 62: Order Fulfilment process & functionalities - Product

PVC (Price Variation Clause) and SVC (Statutory Variation Clause) is also part of Fulfilment. Base price can be changed through PVC and GST can be changed through SVC clause during invoicing. Through which total order value can be changed.
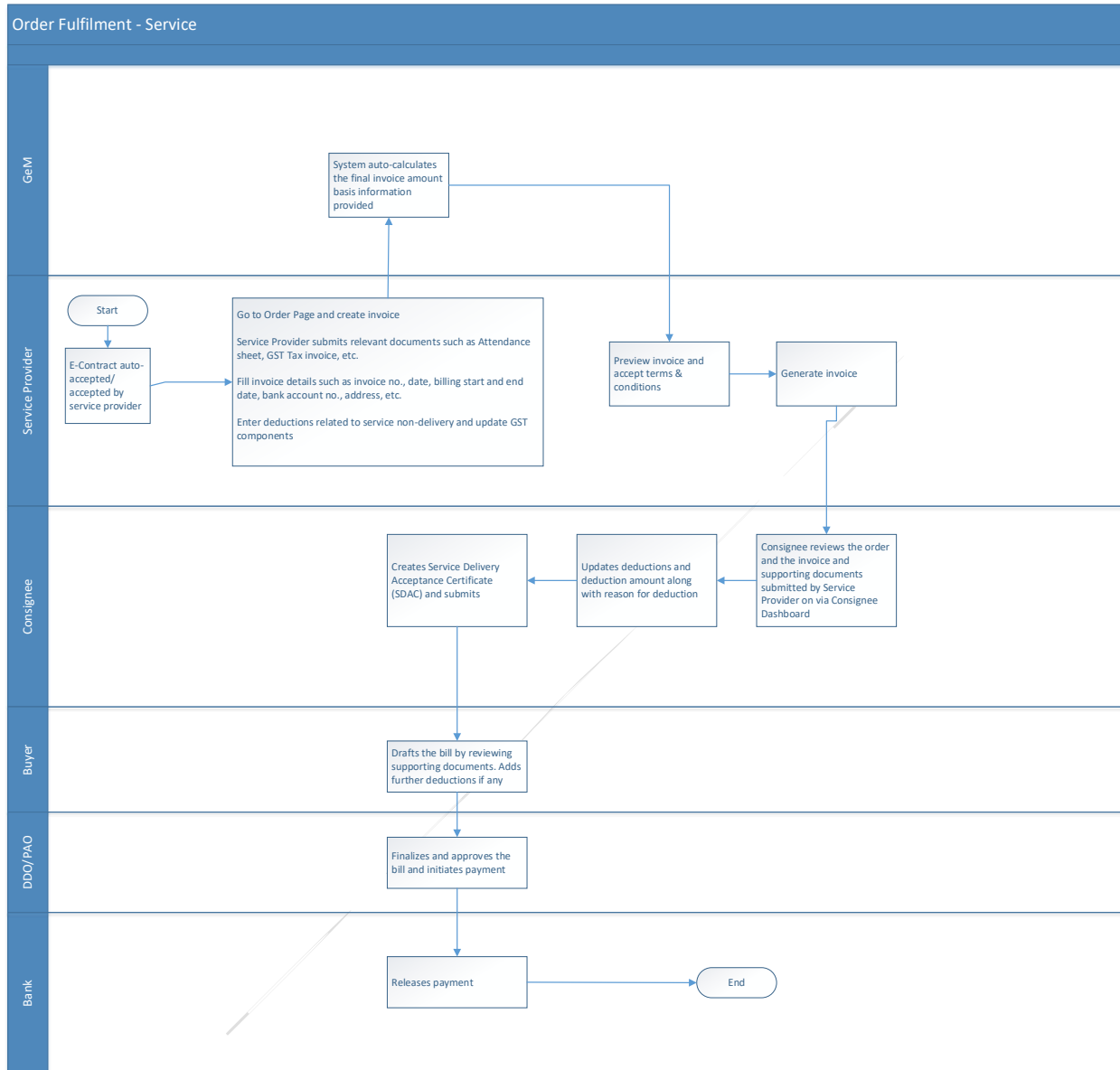
Figure 36: Order Fulfilment - Services

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Service provider goes to the Order Page and creates invoice: 1. Service Provider submits relevant documents such as Attendance sheet, GST Tax invoice, etc. 2. Fills invoice details such as invoice no., date, billing start and end date, bank account no., address, etc. 3. Enters deductions related to service non-delivery and update GST components	1.1	Invoice generation form with document upload functionalities and editable fields
2	System auto-calculates the final invoice amount basis information provided	2.1	Auto-calculation of final invoice amount
3	Service Provider previews invoice and accepts terms & conditions and generates the final invoice	3.1	Generate invoice PDF using input information and documents
4	Consignee reviews the order and the invoice and supporting documents submitted by Service Provider on via Consignee Dashboard	4.1	Consignee Dashboard View with details pertaining to all orders including invoice and supporting documents uploaded by Service Provider
5	Consignee updates deductions and deduction amount along with reason for deduction and creates and submits the SDAC	5.1	Functionality for SDAC creation and generation
6	Buyer drafts the bill by reviewing supporting document and adds further deductions if any	6.1	Buyer Dashboard with view of all bills. Functionality to edit and save draft bills basis review of supporting documents (invoice, financial approvals, SDAC, sanction order, etc.)
7	DDO/ PAO finalizes and approves the bill and initiates payment		

| 8 | Payment released from Buyer's account | 8.1 | Integration with payment systems such as PFMS, IFMS, GPA, etc. to enable blocking and releasing of payments |
| | | 8.2 | Incident dashboard to raise and manage incidents |

Table 63: Order Fulfilment process & functionalities - Services

8.1.8.1   Additional interventions/ functionalities required:

1. HSN code can be integrated with GSTIN portal through which updated GST rates can be captured for SVC cases

2. Provision for Buyer to close the order if:

    a. only <5% of the quantity has not been fulfilled by the Seller

    b. >=95% of the quantity fulfilled has been accepted by the Buyer *(currently ongoing)*

3. Functionality for configurable time period for PRC and CRAC generation

4. Transaction charge in case of services to be collected before the invoice generation *(currently ongoing)*

5. Functionality to capture ITC pertaining to GST in invoicing *(currently ongoing)*

6. Provision to capture base price of products/ services and breakup of taxes, including GST, separately in invoicing

7. For any service procured via Forward Auction, appropriate invoicing and post contract management processes shall be developed and implemented

8.1.9 Payments

8.1.9.1   Outgoing payments (Buyer to Seller/ Service Provider):

The payments from Buyer to Seller/ Service Providers might include payment for orders, staggered payments in case of services, etc. The Buyer will have multiple options for making the payment:

1. PFMS

2. IFMS

3. GeM Pool Account (GPA)

4. Online payment via payment gateways: GeM has integration SBI MOPS to facilitate Buyers/ Sellers/ Service Providers who are using payment gateways for internet banking, corporate net banking, RTGS and NEFT, etc.

5. Dedicated integrations with Indian Railways, CGDA, CRPF systems for payments

6. ERP based payment systems: The bill data is pushed to Buyer ERP systems, CPSUs pay via their own systems, and shares payment status with GeM (e.g., IOCL, ONGC, SAIL, BHEL, etc.)

The following section provides a detailed view of the various outgoing payment methods available on GeM and the system functionalities needed to enable the process.

8.1.9.1.1   Registration of Payment Method:

Before being able to use a particular payment mode to initiate and make payments, the Buyer's primary user needs to select payment mode for the organization at the time of registration.

Post this, in case of PFMS/ IFMS, Buyer's primary user is required to map budget heads to DDOs (part of Buyer registration process).

In case of GPA, the NPAE needs to first open a GPA account with GeM partnered bank. The primary user will link the GPA bank account with GeM by selecting appropriate payment mode and provide bank a/c details, post which the Buyer can operate the account. The registration process for GPA is described in detail in the below section.

8.1.9.1.2   Bill generation:

Prior to initiating any payment, Buyer is required to generate the final bill (payment sanction cum bill), which is then approved by the DDO/ PAO. Following is the process for final bill generation:
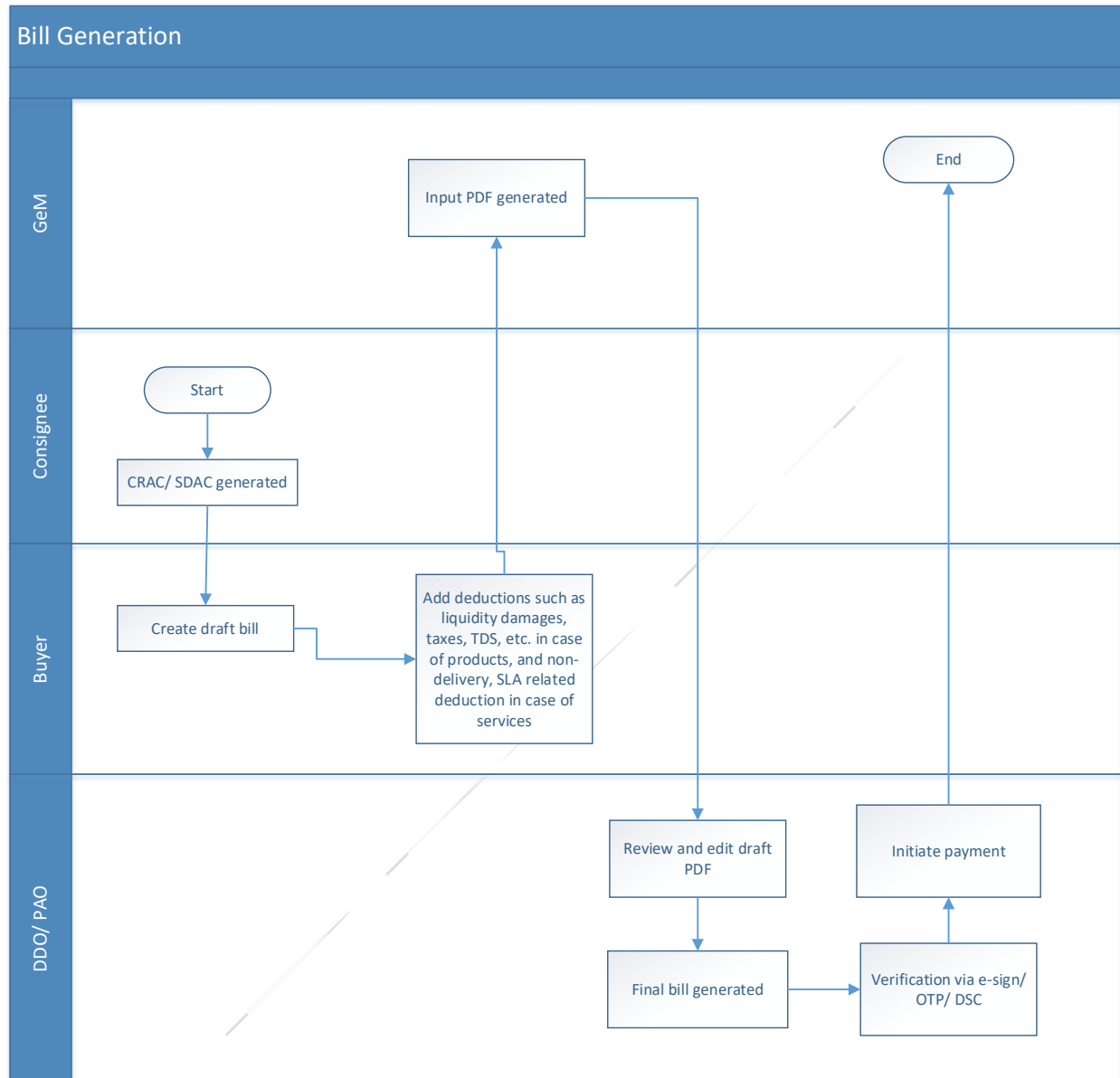
Figure 37: Bill Generation

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Secondary user at the Buyer side generates CRAC/ SDAC		
2	Buyer creates a draft bill basis the product quantity accepted as per CRAC, and the service accepted as per SDAC. He/ she then adds the deductions such as Liquidated Damages if any, taxes, etc. in case of product, and non-delivery and SLA related deductions in case of service		
3	Post this an input PDF is generated and reviewed and edited by the DDO/ PAO	2.1	Bill PDF generation
4	Once the DDO/ PAO finalizes the draft, he/ she generates the final bill and verifies it via e-sign, OTP or DSC. Once this is done, Buyer can now initiate payment to the Seller/ Service Provider	3.1	Functionality to enable digital signature / e-Sign based authentication
		3.2	Trigger OTP for verification to Seller/ Service Provider & verify using the input

Table 64: Bill Generation process & functionalities

In case of services contract, the bill can be generated multiple times as per payment timelines.

8.1.9.1.3 PFMS/ IFMS:

Central and state governments can use PFMS or IFMS respectively by selecting the appropriate budget head. GeM will block the budget as per the order payment to be made (in case of products) and equal to the amount for 2 billing cycles on a recurring basis for every billing cycle (in case of services) and once the bill is pushed to the PFMS/IFMS system, the payment will be released and reflected on GeM post appropriate checks

The payment process via PFMS/ IFMS broadly consists of the following steps, described in detail below:

1. Fund blocking prior to successful order creation (optional for orders with delivery period greater than 15 days - these limits are subjected to change as per Payment OM issued by Department of Expenditure and hence, should be configurable for GeM to modify as needed.)

2. Fund unblocking in case of order cancellations

3. Order data made available for pull by IFMS system for payment purposes

4. Payment via PFMS/ IFMS and payment status displayed on GeM

Fund Blocking
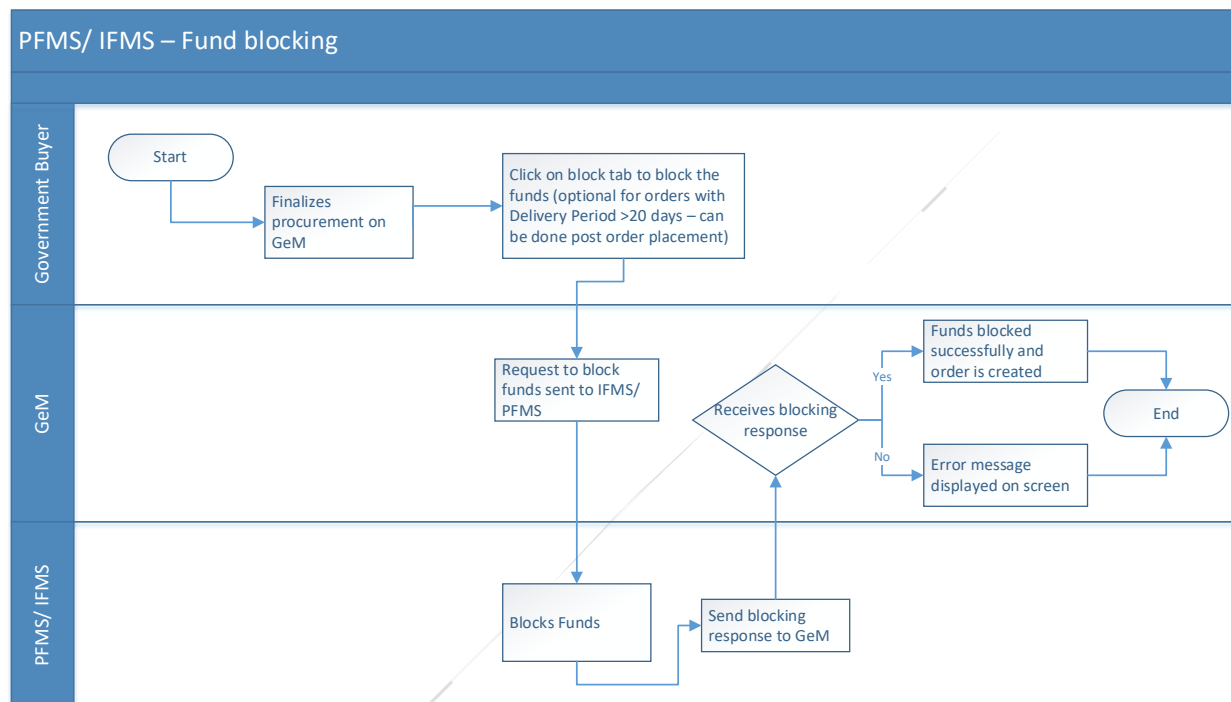
Figure 38: Fund blocking

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyer finalizes the procurement on GeM portal and clicks on 'Block' tab to block funds post which GeM raises a request to IFMS/ PFMS system to block the funds	1.1	Integration with IFMS/ PFMS

2	PFMS/ IFMS blocks funds and sends a response back to GeM. In case of success, order is created successfully. In case not, an error message is shown	2.1	Error message upon failure of fund block

Table 65: Fund blocking process & functionalities

Fund Unblocking

There are multiple reasons that can lead to the need for unblocking the funds previously blocked. Some of the reasons include:

1. Order cancellation

2. Partial delivery of order

3. Deductions such as Liquidated Damages, SLA and non-delivery related deductions in case of services, etc.

4. Quantity amendments

5. Contract amendments/ cancellation

6. Partial closure of order

7. Demand cancellation

8. Cross financial year payment (budget lapsed with the end of financial year)
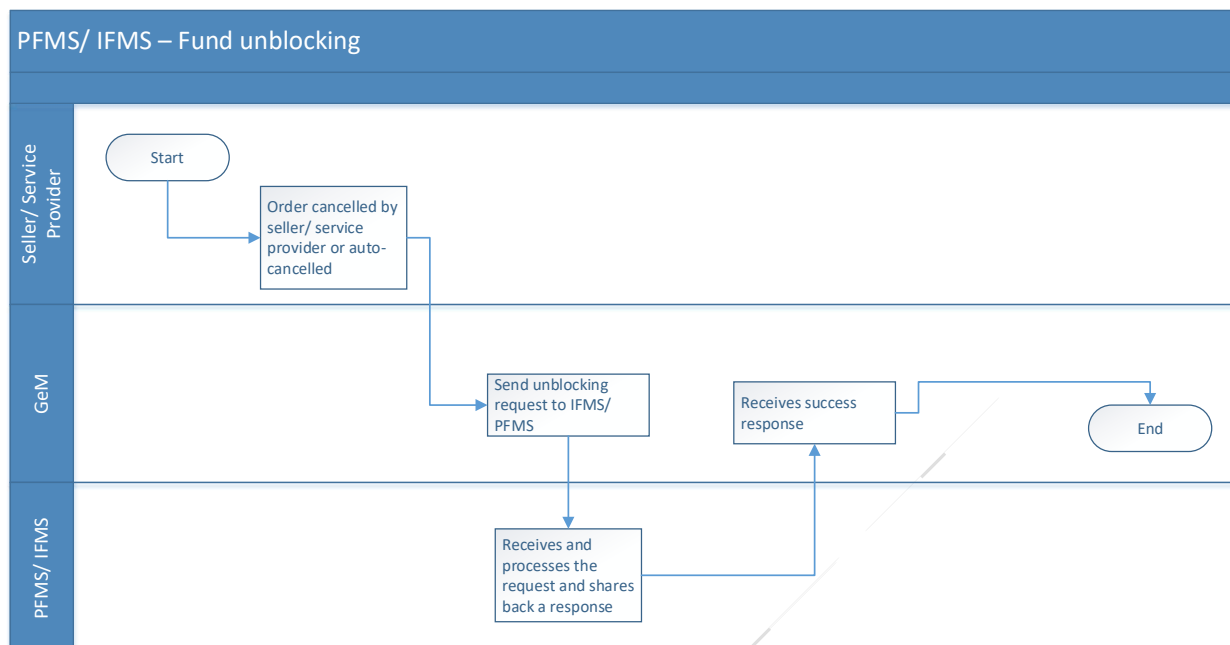
Figure 39: Fund unblocking

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	In case an order is cancelled by the Buyer/ Seller/ Service Provider/ Buyer or auto-cancelled, GeM sends an unblocking request to IFMS/ PFMS	1.1	Integration with IFMS/ PFMS
2	IFMS/ PFMS processes the request and shares status with GeM		

Table 66: Fund unblocking process & functionalities

Order Data Pull (only IFMS and select ERP systems)

Order data is shared with select ERPs and few IFMS integrations as the entities want to update/feed the data in their system as well.
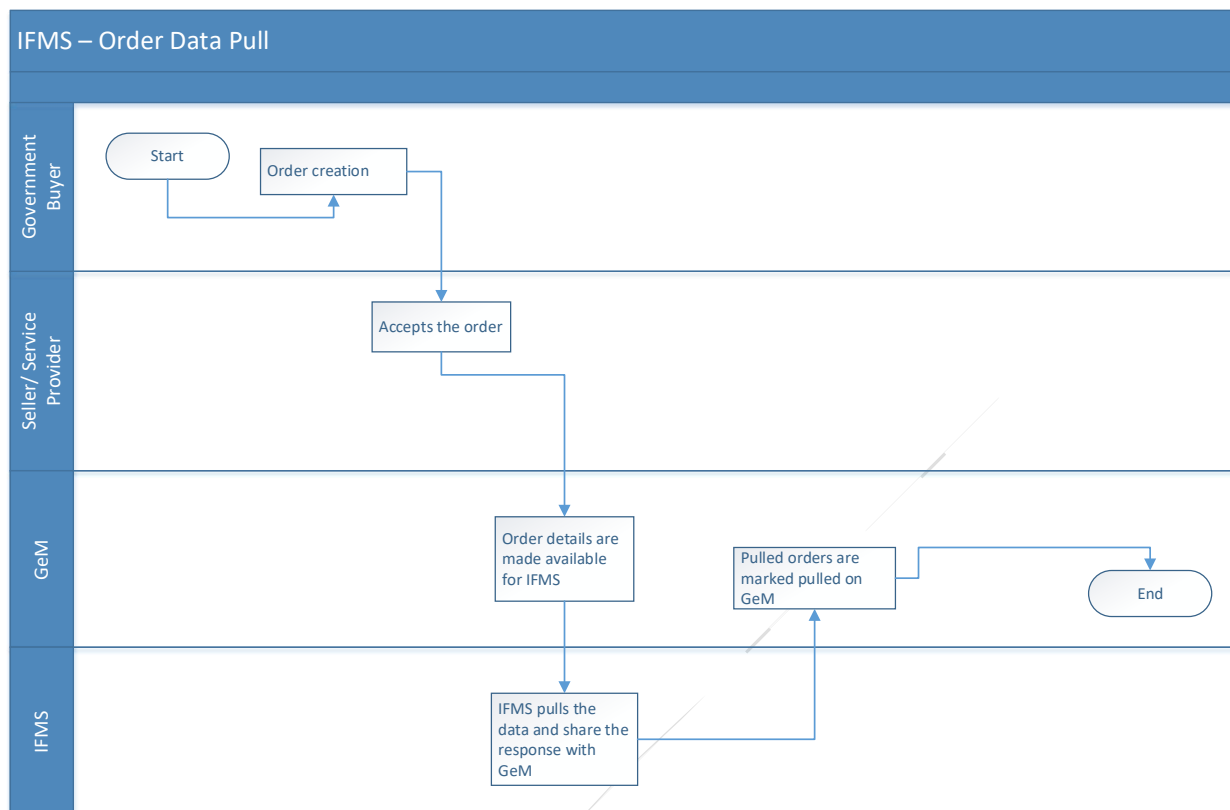
Figure 40: Order Data Pull

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Upon order acceptance by Seller/ Service Providers, order details are made available by GeM to IFMS	1.1	Integration with IFMS
2	IFMS pulls the data and shares the response with GeM		
3	Pulled order data is marked pulled on GeM upon receiving the response from IFMS	3.1	Order data pull marked complete once information received from IFMS

Table 67: Order data pull process & functionalities

Payment via PFMS/ IFMS
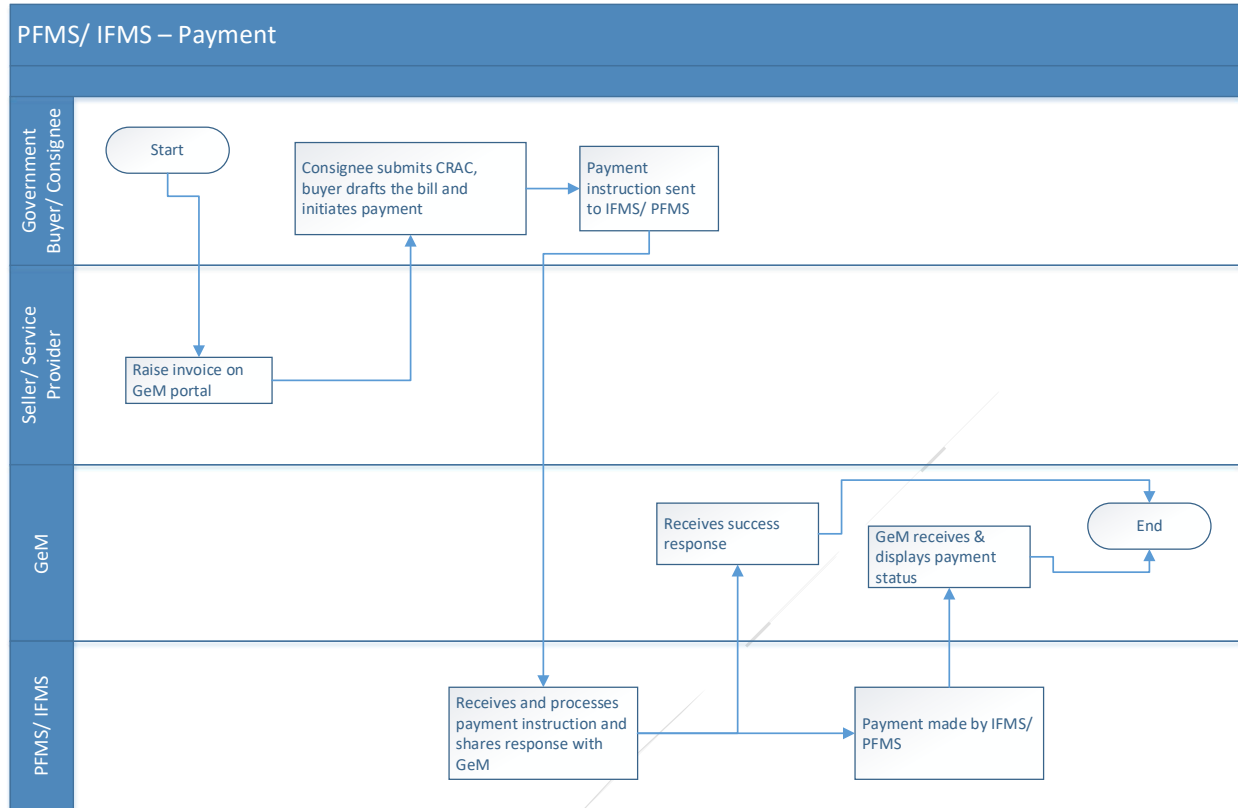
Figure 41: Payment via IFMS/ PFMS

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Seller/ Service provider raises an invoice on the GeM portal	1.1	Generate invoice PDF using input information and documents
		1.2	Functionality to enable digital signature / e-Sign based authentication
		1.3	Trigger OTP for verification to Seller/ Service Provider & verify using the input
		1.4	Integration with ERP systems of select Buyers

		1.5	Store collected documents on cloud
2	Post raising of invoice and submission of proof of delivery by Seller, consignee completes PRC and CRAC generation, post which Buyer creates a bill and initiates payment by sending instruction to IFMS/ PFMS	2.1	Trigger notification to consignee at appropriate time period
		2.2	Auto-generation and verification of PRC and CRAC post defined timelines after invoice and proof of delivery submission
3	IFMS/ PFMS receives the payment instruction and send a success response to GeM for payment being initiated	3.1	Integration with IFMS/ PFMS
4	IFMS/ PFMS completes payment and shares the status with GeM which then displays the status on the portal		

Table 68: Payment via IFMS/ PFMS process & functionalities

8.1.9.1.4   GPA:

GPA is a special purpose bank account opened, operated, and controlled exclusively by each NPAE (Non-PFMS Agencies/Entities) for the purpose of crediting projected value of the contracts/supply orders into the account and for subsequently making timely payments to the Sellers/ Service Providers on successful supply and acceptance of goods & services ordered on GeM against supply orders placed by the NPAE on GeM. The credit process in GeM pool account differs for products & service orders as below.

1. Product Orders: Buyers are mandated to credit 100% of the projected order value before the order creation, for contracts with delivery period up to 20 days. For contracts with longer delivery periods, fund blocking of appropriate amounts shall be initiated at a date 20 days prior to expected delivery date or on the date of invoice generation by the Seller in GeM whichever is earlier. These limits are subjected to change as per Payment OM issued by Department of Expenditure and hence, should be configurable for GeM to modify as needed.

2. Services Orders: Buyer are mandated to credit funds in GeM Pool Account as per the services billing cycle. The funds will be equal to projected value of service order as per 2 billing cycles.

Before using GPA to make the payments, the Buyer needs to top-up the account, which can be done in two ways:

1. Challan: Buyer can generate challan through bank to get funding for the payment that is due.

They can then submit the challan in the bank account and the payment will be blocked and then released post consignee confirmation.

2. Non-challan: No specific funding is needed, and the Buyer can top-up the account with a lumpsum amount. For every payment due, the payment amount will be blocked from the total amount and will be released once the bill is generated

To facilitate the payment process GeM has integrations with PFMS, IFMS, SBI MOPS, and select banks to that enables GeM to support the following sub-processes:

1. Bank account verification

2. Secondary user mapping

3. Balance inquiry

4. Fund blocking and unblocking

5. Challan generation

6. Payment API and status sharing

Onboarding process
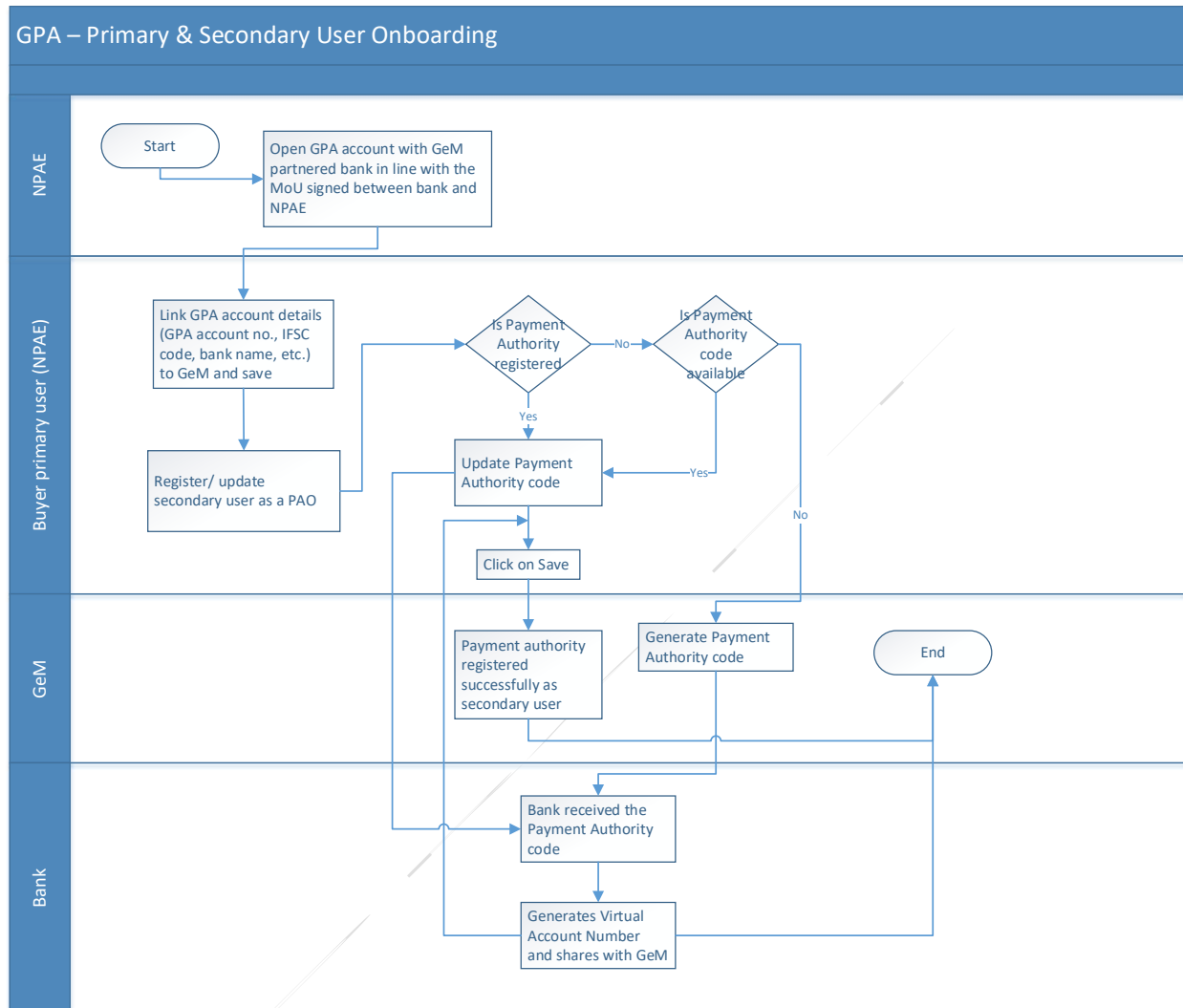
Figure 42: GPA Primary & Secondary User Onboarding

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	NPAE should open a GPA account with GeM partnered bank in line with the MoU signed between bank and NPAE. Post this, primary user must link the account to GeM		
2	Post linking GPA with GeM, primary user can register/ update a secondary user as a PAO. In case a payment authority is already registered, primary user must update the payment authority code and click on save	2.1	Map secondary user (PAO) to primary user and organization hierarchy
3	In case payment authority is not registered, if a payment authority code is available then primary user can simply register the PAO and update the payment authority code on GeM. In case payment authority code is not available, then it needs to be generated via GeM	3.1	Trigger Payment Authority code generation
4	Bank receives the payment authority code and generates a Virtual Account Number against the payment authority code and shares it with GeM. Post this the bank a/c can be used by the Buyer	4.1	Integration with Bank systems and select ERPs (to enable sharing of data)

Table 69: GPA Primary & Secondary User onboarding process & functionalities

GPA Account Funding via Challan Mode and Order Placement
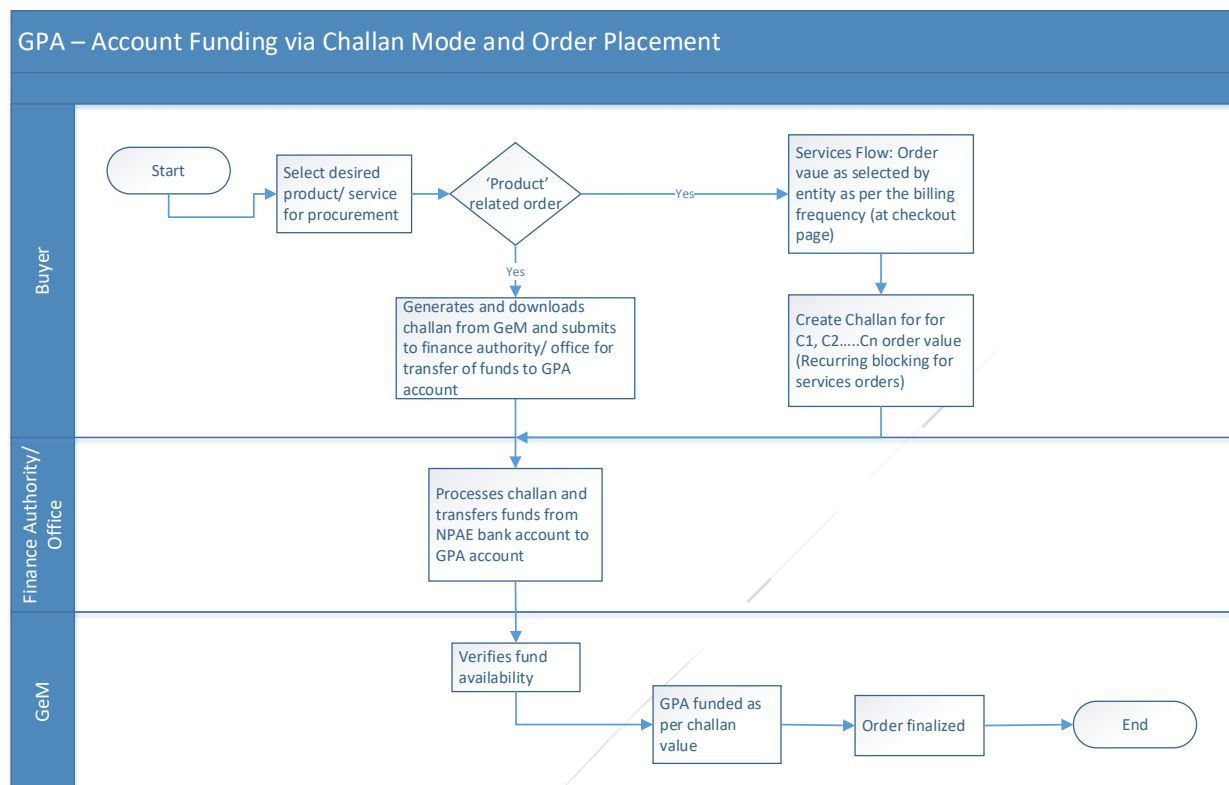
Figure 43: GPA Account Funding via Challan Mode and Order Placement

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	Buyers selects desired product/ service. In case it is a product related order, Buyer generates and downloads Challan from the GeM portal and submits it to a finance authority/ office to transfer relevant funds to the GPA account	1.1	Redirect Buyer to bank system where t he/she can generate the challan and download it for further payment
2	Post the transfer is complete, GeM verifies the fund availability. If the GPA is funded as per challan value, order is placed	2.1	Integration with bank systems for trigger balance enquiries & verification

| 3 | In case of services order, recurring blocking is permitted as per payment frequency. For each payment, Buyer needs to generate and submit the challan for transfer of funds to GPA account as described above. After GeM verifies the account balance, the services order is finalized | | |

Table 70: GPA Account Funding via Challan Mode and Order Placement process & functionalities

GPA Account Funding via Non-Challan Mode and Order Placement

In case of funding via Non-Challan Mode, the Buyer funds the GPA account with a certain amount at the time of their choice, rather than prior to every order placement. Prior to placing the order, the system checks if the total amount in the account is greater than the order value (in case of products) or amount for 2 billing cycles (in case of services). In case there is sufficient balance in the account, the funds are blocked, and the order is placed.

Payment via GPA
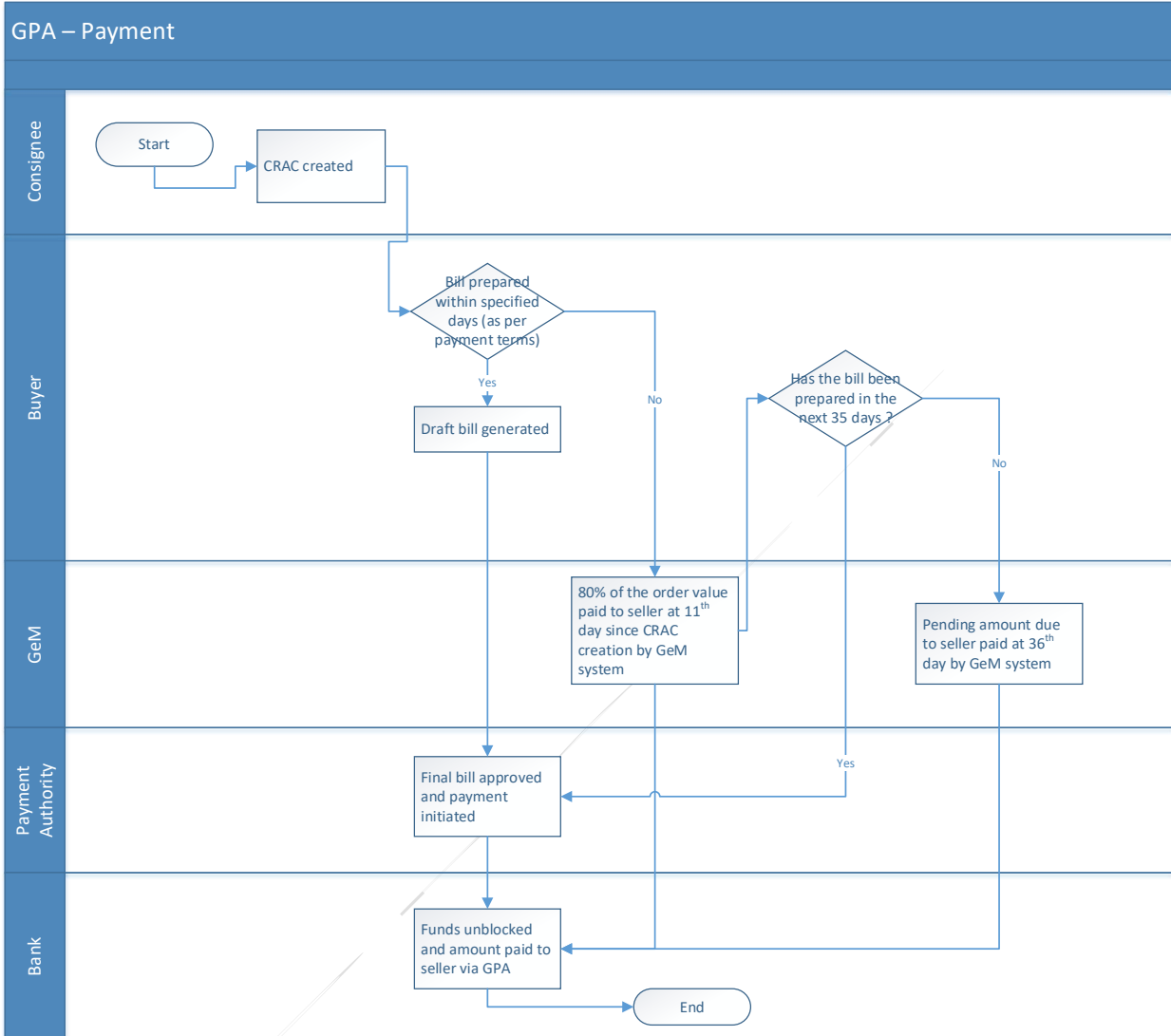
Figure 44: GPA Payment

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Once the consignee creates the CRAC, Buyer has 10 days to prepare a draft bill. In case	1.1	Automated workflow for approval of bill generated

	the Buyer generates the draft bill within timelines, payment authority registered with GeM approves the bill and initiates the payment		
2	In case Buyer doesn't generate the bill within 10 days, GeM automatically pays 80% of the order value to the Seller on the 11th day since CRAC creation	2.1	Trigger to initiate 80% of payment basis rule engine
3	In case Buyer doesn't create the bill within 35 days of CRAC creation, GeM pays the pending amount to Seller on the 36th day since CRAC creation	3.1	Trigger to initiate remaining payment basis rule engine
4	Post this the amount is unblocked and paid to Seller from the GPA	4.1	Integration with bank system

Table 71: GPA payment process & functionalities

8.1.9.1.5 Additional Payment Integrations – CGDA, CRPF, Indian Railways, etc.

CGDA: CGDA is the point of integration between the Ministry of Defence and GeM for the processing of all the payments to the Sellers. GeM shares the Bill details with CGDA for all the products/ services procured on GeM by the Buyers registered under Ministry of Defence. CGDA would share the Payment status with GeM once the payment is processed for the bills generated on GeM.

CRPF: CRPF (Central Reserve Police Force) is a central government organization under Ministry of Home Affairs. CRPF buying on GeM was around 1000 Cr for the current financial year. CRPF payments are being processed by PFMS (Public Financial Management System) which is a web-based online software application developed by Controller General of Accounts (CGA), Department of Expenditure, Ministry of Finance.

GeM has an integration with CRPF SELO (Service & Loyalty) and PFMS customized application to facilitate the CRPF Buyers to process their procurements and payments on GeM portal. The GeM has introduced CRPF Online payment mode for CRPF Buyers. Aim of this integration is to ensure that Buyers use their allocated budgets only and only those orders are processed on GeM which have budget availability in SELO & PFMS. The scope of this integration is to get the real budget allocated to a Buyer through CRPF SELO and reconciliation of Bills.

As per the DoE (Department of Expenditure), every central government organization is to block the fund before the order placement on GeM portal. CRPF Buyers process their fund request first on SELO CRPF Application and then through PFMS application for final blocking of fund processing of order. If Buyer cancels the order or declines the demand mid-way, then

same way unblocking of fund on GeM portal can be done. Firstly, through PFMS and then afterwards on SELO & GeM portal.

In some cases where delivery is beyond 20 days, CRPF Buyers process their fund blocking request at the time of bill generation. Since there is fund blocking is required at the time of order placement, in such cases, CRPF Buyers choose other payment mode on GeM at the time of order creation and process their bills online through PFMS and updating on GeM.

Apart from above, CRPF Buyers also have the provision to unblock the fund in terms of cancellation of demand/order, partially executed orders (partial unblocking of fund) and bills returned from PFMS.

The following APIs have been used with CRPF SELO Application - Blocking on Fund, Unblocking of Fund and GeM Bills Sharing. Apart from APIs, email notifications to be sent on daily basis for status of bills consumed by CRPF Web Service on a particular day.

MoPR: Integration with e-GramSWARAJ (eGS) to enable the Panchayats to procure goods and services through GeM leveraging the eGS platform. It is the endeavour of Ministry of Panchayati Raj (MoPR) that all procurement of goods and services by Panchayats may be done through GeM. MoPR has already developed an end-to-end application called e-GramSWARAJ for capturing end to end activities of the Panchayats (Profile, Planning, Progress Reporting and Accounting etc.). Integration between eGS and GeM enables Panchayats to procure through GeM. Panchayats are able to view the concerned vendors along with the pricing from GeM in eGS portal (e.g., if a Panchayat wishes to buy cement, they will be able to search the vendors and select one). Once the vendor and quantity are finalized final rate should be fetched automatically from GeM and shown in eGS. Buyer completes the procurement cycle on GeM. Panchayat makes the payment with the current process through eGSPI (FTO generation and online payment). Expenditure details are then shared with GeM. GeM has already conducted a pilot of this system successfully and is gearing for a full roll out

8.1.9.1.6   Additional interventions/ functionalities needed:

IFMS:

1. Offer IFMS integrations with state systems as a standard functionality/API which can be customized for different entities instead of creating standalone, highly customized instances for each state

2. Robust Buyer mapping to facilitate implementation of auto-payment mode assignment and state-specific buying rules

3. Allow state governments to select the mandatory payment mode for all entities tagged to the respective state

4. Allow the option for partial order closure and partial unblocking of funds in case the Seller is unable to supply the full quantity, or the Buyer doesn't need the pending quantity

5. For quantity amendments, the new order created post quantity adjustment must be mapped to original order no. for reference

6. Budget head master data to be fetched from PFMS/IFMS should be automated and Buyer should also have an option to fetch the latest data

7. Re-blocking of funds on lapse of annual budget/ change of financial year for active orders

PFMS:

1. Re-blocking of funds on lapse of annual budget/ change of financial year for active orders

2. Optional fund blocking functionality enabled at end of financial year

3. Integration with e-Asset ongoing to maintain linkage with Asset Management Repository which captures items CPSUs, and Ministries have purchased

GPA:

1. Scale up the current limit of 3-5 GPA accounts per primary user by multifold

2. One-to-one GPA account mapping at secondary user level

3. Buyer should have option to switch the type of GPA mode: He/she can add both modes during registration process and while order placement he/she should have flexibility to select the mode (Challan/ Non-Challan)

4. Online cancellation of Challan via GeM portal and integrations with bank

Additional Payment Integrations - CGDA, CRPF, Indian Railways, etc.:

1. Functionality to facilitate process to ensure payment in cases where bills are returned by payment authority to Buyers in case of Indian Railways *(currently ongoing)*

Overall:

1. Provide additional features such as an option to retry a payment in case of payment failure

2. Automated unblocking of funds in case order is cancelled

3. Option to edit budget heads via GeM portal in case of error in mapping

4. Error codification and standardization to ensure streamlined communication of errors such as Seller account wrong, IFSC incorrect, etc.

5. Modify bill generation process - once Buyer generates the CRAC/ SDAC, Seller/ Service Provider shall file a claim for payment, post which Buyer shall proceed with generating the draft bill

6. Provision to capture base price of products/ services and breakup of taxes, including GST, separately in bill generation

7. E-Wallet functionality for Sellers/ Service Providers to ensure payments from Sellers/ Service Providers (e.g., transaction charges, caution money deposit, etc.)

8. Payment initiator role to be created for Buyers for draft bill generation

8.1.9.2 Incoming Payments from Seller/ Service Provider or Buyer to GeM:

GeM platform will navigate Sellers/ Service Provider to the Payment Gateway/Aggregator (SBI MOPS). The Seller/ Service Provider will make online payments for caution money, transaction charges, Annual Milestone charges, interest charges in case of delayed payments as applicable, using card/net - banking, IMPS/wallet-based payments.

8.1.9.2.1 Caution Money Deposit:

GeM platform allows the Buyers to place an order to Sellers/ Service Providers for their requirement of Goods or services. To ensure there is a certain ownership of the Sellers/ Service Providers for products/services listed in marketplace, specifically catalogue and fulfilment, mechanism of caution money bearing financial penalty to Sellers/ Service Providers has been devised albeit in measured proportion.

Sellers last year's IT turnover would be taken for calculation of amount of Caution Money. Calculation of caution money will not change mid-year, i.e., Seller/ Service Provider's present year's turnover will not impact the calculation and only last year's turnover will be taken for calculation. The turnover should be the latest year available from the last 3 years. Sellers/ Service Providers who have not declared their turnover, need to provide an undertaking stating that he/ she hasn't filed any return and hence he/ she has not provided the turnover details on GeM portal.

Caution Money Minimum Deposit Slabs:

Seller Turnover (Rs.)	Caution Money Threshold
<1Cr	Rs. 5000
>=1Cr &<10Cr	Rs. 10000
>=10Cr	Rs. 25000

Table 72: Caution Money

All amount mentioned above are variable and are subjected to change pre or post implementation. Changes in these should not impact overall flow. For a financial year, caution money slabs shall be constant. There would be no maximum limit for caution money deposited by Sellers to GeM. For all cases where there is no turnover, the base fee of lowest slab will be taken as caution money.

Caution money can be deducted as per the Caution Money policy defined by GeM. Some of the key reasons for imposition of a penalty include:

1. Cancellation/rejection of Direct Purchase order by Seller

2. Order cancelled by Buyer for the orders that are not delivered till delivery period and

3. invoice is not generated against that order.

4. Order Cancelled by Buyer after delivery period expiry + 15 days and invoice has been

5. generated by the Seller but order is not delivered

6. Fails to furnish requisite performance security/PBG as per GeM e-bid/RA conditions

Following is the detailed process of caution money deposit:
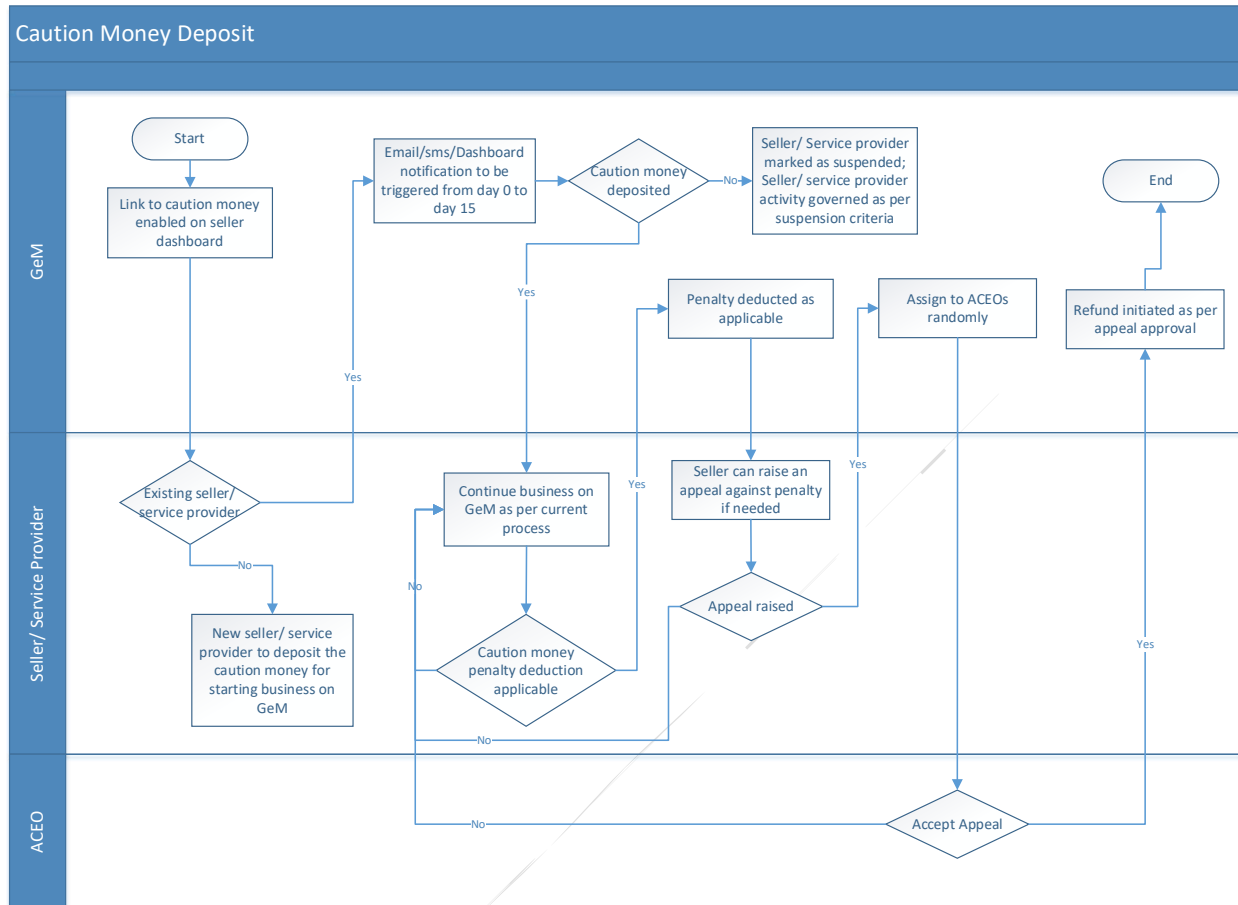
Figure 45: Caution Money Deposit

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	In case of a new Seller/ Service Provider registered on GeM, a message/notification will be shown post registration to the new Seller's dashboard regarding the Caution Money- deposit, deduction, timelines, and all relevant policy details	1.1	Periodic notifications to Sellers/ Service Providers via email and SMS
2	Seller/ Service Provider will need to mandatorily deposit the caution money via	2.1	Online payment integrations (SBI MOPS) and integrations with banks

	online payment options available before doing anything on GeM portal. Upon payment confirmation, Seller will be able to resume normal operations on GeM portal like uploading products, receiving orders and participation in bids as soon as payment confirmation is received from the bank	2.2	Rule based engines to allow Seller/ Service Provider to use all relevant functionalities of GeM portal once caution money has been deposited
3	In case of an existing Seller/ Service Provider, from" Day T0 to Day T0+15 (configurable), e-mail/SMS and Seller dashboard notification will be sent to all Sellers with active catalogue in marketplace informing them regarding the Caution Money- deposit, deduction, timelines and all relevant policy details.	3.1	Periodic notifications to Sellers/ Service Providers via email and SMS
4	A 'link' to deposit the Caution Money as per their 'turnover slab' will get enable on the Seller Dashboard in order to deposit the Caution Money by Sellers. Seller can deposit any amount above the Caution Money Threshold ('M'), deduced as per latest turnover details available with GeM	4.1	Auto-calculation and generation of caution money payment link
5	On T0 +16th day, all Sellers with less than the minimum amount (M) as Caution Money will be treated as a suspended Seller Following criteria is applicable for the suspended Sellers: 1. Seller will not be able to upload new brand / products 2. Will not be able to participate in new Bid 3. Buyers will not be able to place Direct Purchase/L1/BID/RA against suspended Seller's products 4. Existing Direct Purchase / L1 / Bid/ RA orders continues as it is, system	5.1	Rule based engine to restrict functionality for suspended Sellers/ Service Providers

	will not stop by fulfilling the orders to Buyers	
	5. Acceptance/Rejection of existing Direct Purchase / L1 placed orders continue as it is	
	6. Any existing BID/RA in which Seller has participated will continue as it is	

Table 73: Caution Money Deposit process & functionalities

As per current process, caution money shall be refunded in the following situations:

1. **Caution Money Refund of Excess Funds**

   The Seller/ Service Provider would have the option to transfer the Excess funds if any from their caution money account to the one specified in their GeM profile. The excess funds are any amount of funds over and above the caution money threshold amount of the Seller/ Service Provider. The Seller/ Service Provider would get the option on GeM portal to withdraw the excess funds. The GeM portal would calculate the excess amount of the Seller/ Service Provider and send the instruction to the Bank to Transfer the Funds from the GeM escrow account to the bank account (The Bank account specified by the Seller in their GeM profile as Primary account would be used as a beneficiary account in this case.) The details of such account would be shared by GeM to the concerned Bank in Refund request.

2. **Caution Money Refund in case of Seller/ Service Provider Account Closure**

   The Caution Money would be refunded back to the Seller/ Service Provider upon their account closure. As a first step system will check whether the Seller/ Service Provider has any contracts pending. In case there are no pending contracts, system will initiate the refund. GeM will send the instruction to the Bank to Transfer the complete amount in Seller/ Service Provider's caution money account to the Seller/ Service Provider's selected bank account. (The Bank account set as primary in the Seller/ Service Provider's profile on GeM at the time of account closure shall be used as the Beneficiary account.) Along with the Transfer of funds, the Bank would also close the Seller/ Service Provider's virtual account.

8.1.9.2.2   Transaction Charges and Annual Milestone Charges:

As per GeM's policy, Seller/ Service Providers are liable to pay GeM the following:

1. A one-time charge titled "Annual Milestone Charge" shall be levied @ 0.5% on all Sellers/ Service Providers clocking a threshold Seller Merchandise Value of INR 20 Lacs in a Financial Year

2. For Sellers who have clocked the threshold Seller Merchandise Value, Transaction Charge at following rates shall be levied on all orders equal to or exceeding Rs. 5 Lacs value in each case:-

Product/Service Order value	Transaction fee Slab
>= 5Lacs but <50Cr	0.5% of order value
>= 50Cr but < 100Cr	25 Lakhs + 0.4% of value above 50Cr
>=100Cr but < 200Cr	45 Lakhs + 0.3% of value above 100Cr
>= 200Cr but <300Cr	75 Lakhs + 0.2% for value above 200Cr
>= 300 Cr but <500 Cr	95 Lakhs + 0.1% of order value above 300 Cr
>= 500 Cr	115 Lacs Flat Fees

Table 74: Transaction Fee

Kindly note that this is the current transaction model slabs and shall be provisioned for customizable thresholds and payment slabs that can be changed as needed by GeM.

Transaction Charges Deposit Process

Following is the process flow for deposit of transaction charges and annual milestone charges:
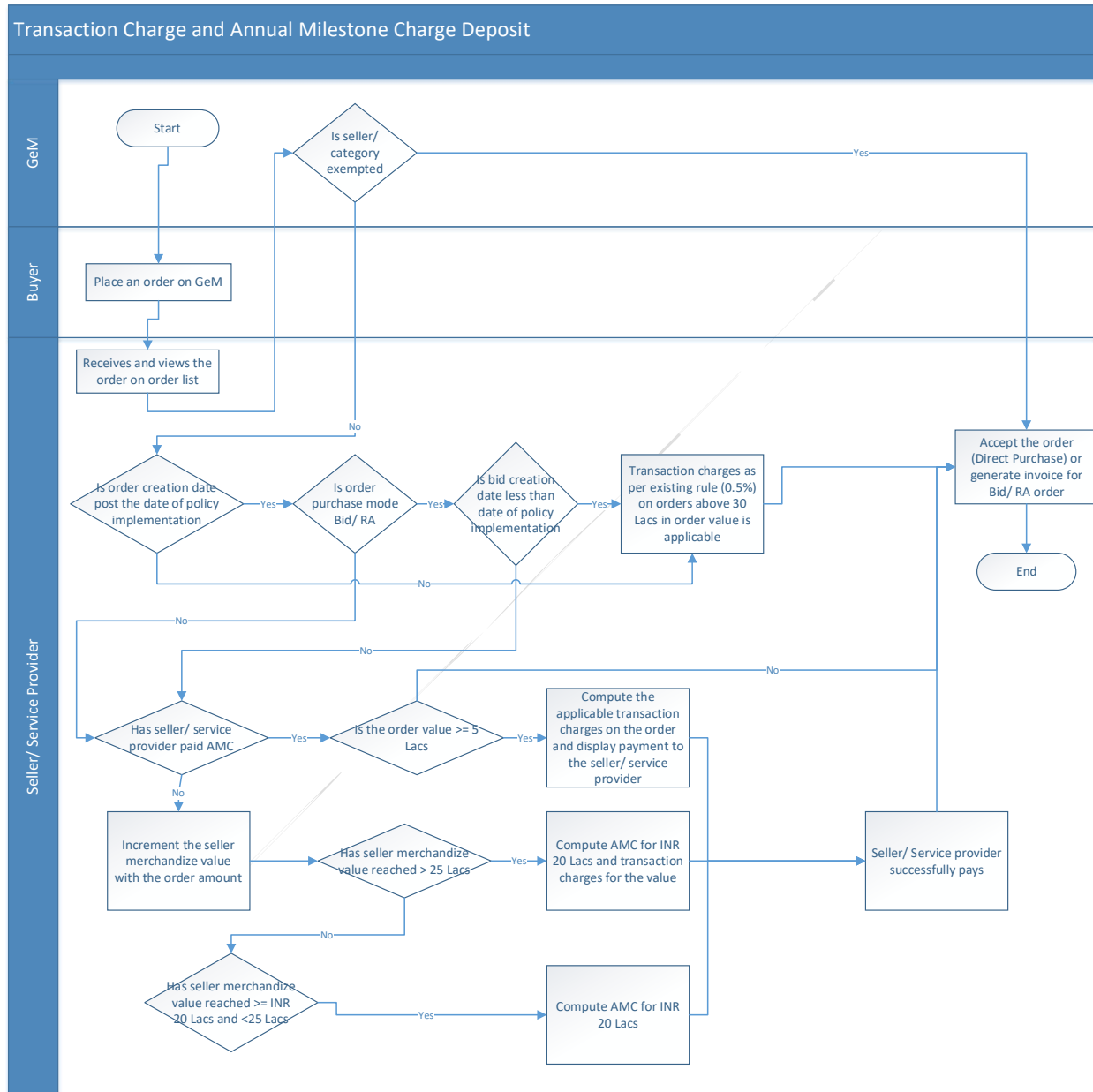
Figure 46: Transaction Charges and Annual Milestone Charges Deposit

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Buyer places the order on GeM and Seller/ Service Provider accepts it. In case the Seller/ Service Provider or the category is not exempted from the charges, the system checks for the order creation date. In case the date or order creation is prior to the date of new revenue policy implementation, transaction charges as per previous revenue policy are levied. In case the date is post the date of new policy implementation, the system checks if the order was placed via Bid/ RA mode and if the bid/ RA was created prior to new policy implementation, in which case the transaction charges as per old policy will be levied	1.1	System prechecks to ensure appropriate revenue policy is implemented basis order creation date, bid/ RA creation date, etc.
2	In case the bid/ RA was created post the date of new policy implementation, system checks if the Seller has already paid AMC. In case yes, system calculates the transaction charge for the order which is then paid by the Seller/ Service Provider via payment gateways	2.1	System pre-checks and rule-based charges calculation
3	In case the Seller/ Service Provider has not yet paid the AMC, the system calculates the total merchandize value of the Seller/ Service Provider. In case it exceeds INR 25 Lacs, Seller/ Service Provider needs to pay appropriate AMC and transaction charges. In case the merchandize value is >= INR 20 Lacs but <INR 25 Lacs, then Seller/ Service Provider is required to pay appropriate AMC		
4	Once the Seller/ Service Provider pays the appropriate charges, they can	4.1	Payment gateway integrations and integration with banks

		4.2	Payment success notification via email and SMS
proceed towards order fulfilment and invoice generation			

Table 75: Transaction Charges and Annual Milestone Charges Deposit process & functionalities

Certain cases are exempted from the transaction and AMC charges. For example:

Transaction charges are not applicable in the following cases:

1. For orders less than Rs. 5 Lakhs in value

2. For orders which are placed and accepted by Seller before the Seller Merchandise Value (SMV) of Rs. 20 Lakhs is reached

Following category of Sellers are exempted from payment of transaction charges and Annual Milestone charges:

1. ACASH

2. KVIC

3. TRIFED

4. WDO

5. Coir Board

6. CPSE to CPSE transactions

The orders placed on GeM portal for commission-based services would be exempted from Annual Milestone charges and Transaction charges computation and payment. Also, in certain cases, the Seller/ Service Provider is entitled to a refund. Some of the cases are listed below:

1. Mutual cancellation of contract by Buyer and Seller/ Service Provider

2. Incorrect selection of goods or services by Buyer

3. In case the related order was placed erroneously or by mistake by Buyer

4. Product/service not required or partially required, as a result of which the Buyer

5. Refused some or full quantity of product/service or requested for discontinuation of

service(s) in the middle of contract

6. Consignee not available to receive the product/ service

A Seller shall not be eligible for refund of Transaction Charges in case Buyer cancels contract due to non- fulfillment of any contractual obligations by Seller or due to any omission /misleading /false information provided by Seller/Service Provider on GeM Portal. This will not cause any limitation on the legal and contractual remedies, including any financial recoveries available to the Buyers and GeM Authorities under the terms and conditions of GeM Contracts and/or Policies. In case of partial cancellation, pro-rata refund shall be made to the Seller.

Transaction Charges Deposit Process via BG (for automobile Sellers)

For Automobile Industry, an alternate arrangement is in place where the Automobile Sellers are allowed to pay the applicable Transaction charges in bulk after every 3 months. This arrangement also requires Automobile Sellers to deposit the bank guarantee with GeM as depicted in the process flow below:

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	For Automobile Sellers, the Payment mode for paying transaction charges will be set to eBG. When such Seller accepts the first order on which the transaction charges are applicable, the Seller will be redirected to eBG process to submit the Bank Guarantee to GeM.		

2	The bank Guarantee amount will be the maximum among the following:
	  1. 0.5% of the total Orders received by Seller during the period 1st April 2018 to 30 June 2018
	  2. INR 5 Lacs		

3	On payment of the Bank Guarantee, the Seller will be able to accept the order Second order onwards, the system will check if the transaction charges applicable on the order is within the 80% of eBG amount deposited by the Seller	3.1	System checks if the amount to be paid for transaction charges is within 80% of eBG
4	In case it exceeds the 80% amount, a Payment challan gets generated for the Seller to make payment within 21 calendar days.	4.1	Rule based generation of payment challan
5	Additionally, after every three months, the GeM System will generate the payment invoice containing the details of the orders, NEFT/RTGS details and the transaction charges to be paid for that period. The Payment Invoice will be sent to the Seller registered email ID. Seller will have 21 days to pay the amount	5.1	Auto-generation of payment invoice every three months. Invoice sent via e-mail

| 6 | On successful payment, the GeM Portal will reset the eBG limit by the amount received from the Seller.

In case of non-payment within 21 days, GeM will cash the eBG from bank and inform the Seller. | 6.1 | System based updation of eBG |

Table 76: Transaction Charges Deposit via eBG process & functionalities

Transaction Charges Refund Process

In case of the order cancellation (as mutually agreed by the Buyer and the Seller/ Service Provider), the Seller/ Service Provider is eligible for the refund of transaction charges. However, no refund of transaction charges shall be made in case Buyer cancels contract due to non-fulfilment of any contractual obligations by Seller/ Service Provider or due to any omission /misleading /false information provided by Seller/Service Provider on GeM Portal.

The refund for the transaction charges is initiated automatically if the Buyer has cancelled the order due to specific set of reasons. In case the Buyer has selected other reasons for the cancellation of order, the Seller/ Service Provider can raise a request- "Review Order Cancellation reason" within 15 days from the date of cancellation of order. The Buyer can give comments and approve or reject the request within 30 days from the date request is raised by Seller/ Service Provider. Post the completion of 30 days, if there is no action by the Buyer, the request is considered as 'Deemed Rejected' by system. If the Buyer approves the request, then the refund is initiated. The timelines are subjected to change as per GeM's decisions.
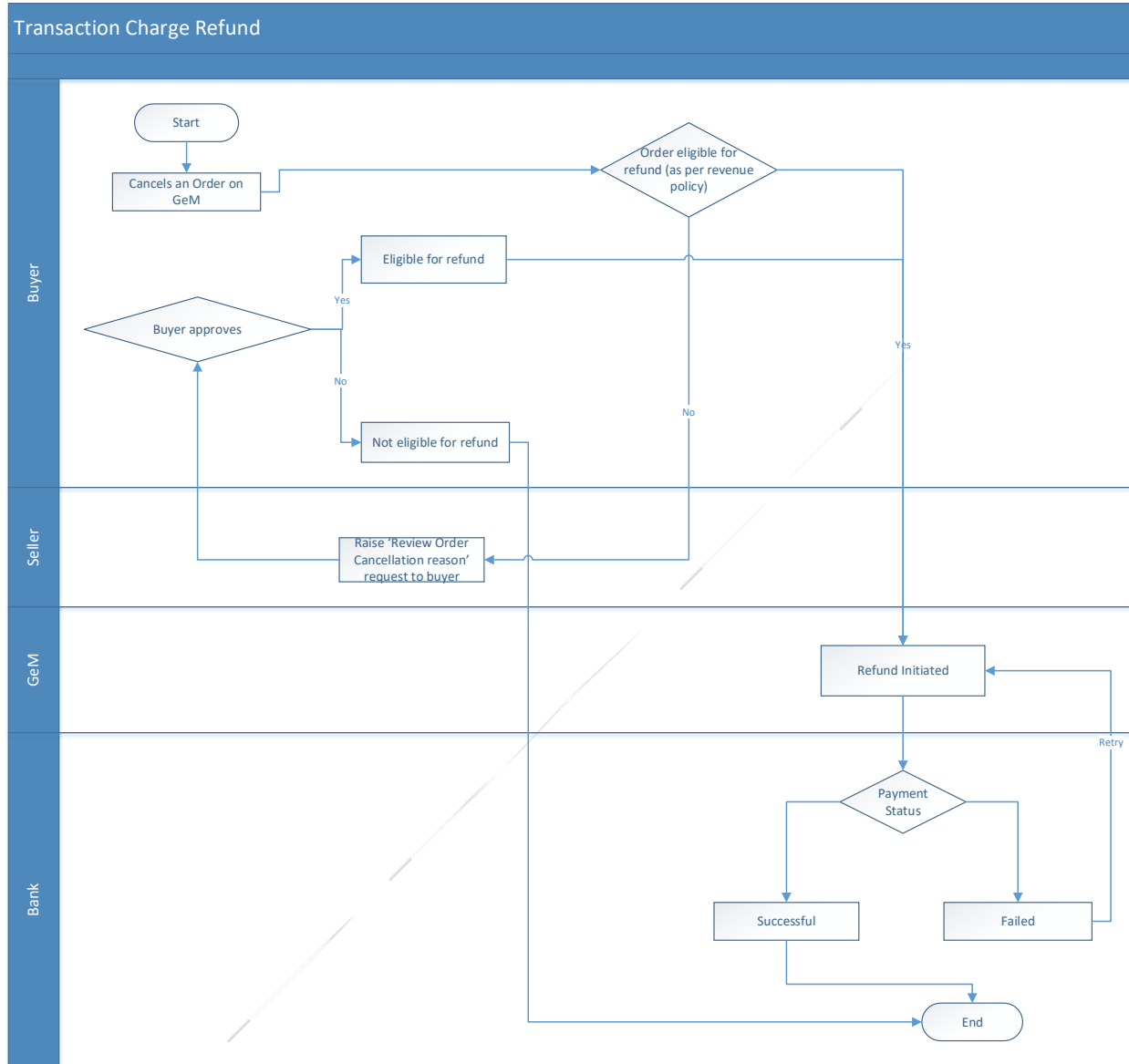
Figure 48: Transaction Charges Refund

Detailed Process Flows			
#	Process Steps	#	System Functionality
1	System will automatically initiate the transaction charges refund if Buyer cancelled the order with the below reasons: 1. Incorrect selection of goods or services by Buyer 2. In case the related order was placed erroneously or by mistake by the Buyer 3. Product/service not required or partially required, as a result of which the Buyer refused some or full quantity of product/service or requested for discontinuation of service(s) in the middle of contract 4. Consignee not available to receive the product/service 5. Any other Administrative reason of Buyer (no default of Seller/ Service Provider)	1.1	System prechecks and rules to ensure automated refund initiation if the order is cancelled by the Buyer due to the reasons mentioned
2	In case the Buyer does not choose the above mentioned reasons while cancelling the order then no auto refund would be initiated. If the Seller/ Service Provider is not satisfied with the order cancellation reason, then they have an option to raise a review request i.e., "Review Order Cancellation Reason" within 15 calendar days from the date of order cancellation.	2.1	"Review Order Cancellation Reason" option
		2.2	System checks to deactivate review option once the timeline has expired
3	Buyer reviews this request and provides the response within 30 calendar days. Buyer can accept/ reject the request. In case Buyer accepts the request, system initiates the refund process. In case of no response from the Buyer in 30 calendar	3.1	Email and Dashboard notification sent to the Buyer for the "Review Order Cancellation Reason" request
		3.2	System checks to identify a response. In case of no response, request automatically marked as "Deemed

	days, the request will be "Deemed Rejected" by the system.		Rejected"
		3.3	Automated refund initiation in case of acceptance of request
		3.4	Integration with banks and payment modes for payment and updation of successful payment status on the dashboard
4	Seller/ Service Provider can view the status of the above request on their dashboard. The credit note would be available for the Seller/ Service Provider to download and will be sent to the Seller/ Service Provider registered email as well.	4.1	Notification on the dashboard
		4.2	Document download option
		4.3	MIS Dashboard for GeM Finance Team to view all such refunds
5	Seller/ Service Provider would not be able to raise the review request again for the same order.	5.1	System checks to ensure only a single request can be raised against an order
6	If a Buyer cancels the order and Seller is eligible for the refund, the refund rules in policy structure are followed (e.g., GST refunded only If the Invoice generation and refund initiation date are in the Current Financial Year)	6.1	Rules based engine to ensure adherence to policy
		6.2	System checks to ensure refund amount dos not exceed the amount of transaction charges paid by the Seller/ Service Provider to GeM.

Table 77: Transaction Charges refund process & functionalities

8.1.9.2.3   Interest Charges in case of Delayed Payments (Buyer to GeM):

For procurements made under rule 149 of GFRs 2017, Buyers are mandated to make payments within 10 calendar days after generation of Consignee Receipt & Acceptance Certificate (CRAC) in the GeM. In order to promote greater discipline and timeliness in payment to vendors by the Buyers, it was decided that whenever a CRAC is auto generated or issued by a Buyer & payment is not made 10 days thereafter, the Buyer organization will be required to pay penal interest @1% per month for the delayed payment beyond the prescribed timeline till the date of such payment. The amount to be paid will be visible to the Buyers on the dashboard.

Buyer will be required to pay interest for every payment delay for every CRAC in full. Partial payment of interest for one CRAC will not be allowed. The Bank will not allow Partial Receipt of challan amount

& manual receipt to be allowed for full payment. Also, the system will not allow to enter partial amount in the given field. Buyer may select multiple line items and pay together. System should keep track of which line item has been paid. Buyer may choose to pay individually for each line item or multiple items together - any number of times he wants to. Buyer may opt to provide a reason for non-payment of a particular line item. System would record the reasons for such non-payments however the line item would continue to remain outstanding against the Buyer. All line items for which interest payment is not made will remain outstanding against the Buyer. Payment Challan & Invoice should be generated for all payments made by the Buyer.

8.1.9.3   Security Deposits (Seller/ Service Provider to Buyer):

The Seller/ Service Provider will pay the EMD, performance guarantee, etc. to the Buyer as applicable. The Seller/ Service Provider can pay the Buyer using an offline Bank Guarantee. In additions to security deposits, Seller is liable to pay tender fee, etc. as well to the Buyer as applicable.

Currently the process of Bank Guarantee deposit is offline, with the Seller/ Service Provider depositing the BG with the bank and submitting the details to the Buyer separately as well as uploading relevant documents on GeM. The Buyer verifies the BG with the advisory bank.

8.1.9.4   Business Cockpit Charges:

Business Cockpit is a user-friendly dashboard that offers a range of value added services to the OEMs on GeM, related to the statistics and insights of their categories. Business Cockpit enables businesses to get deeper insights around value and volume of the business, reseller data, Buyer information, coverage analysis, ratings, etc.

Currently the Business Cockpit has been rolled out with Premium OEM Dashboard version chargeable at INR 600,000 +GST/year. The charges are subjected to change as per GeM's revenue policy.

8.1.9.5   Additional interventions/ functionalities needed:

1. As GeM evolves and grows, there will be a need to scale integrations with banks to facilitate the payment of transaction charges, caution money, etc. further. Currently GeM has integrations with three banks and is in the process to integrate with more banks

2. Scale up payment gateway integrations in the future to facilitate payments

3. Online process for refund of transaction charges in case of situations such as mutual order cancelations

4. Integration with NSDL ongoing to facilitate e-invoice process on GeM

5. Implementation of online EMD process underway

6. Implementation of Online bank guarantee process, via BG on the Go, underway. This will help bring Bank Guarantee related processes such as BG issuance, refund, forfeiture, BG verification, expiry alert to Buyer, etc. online

7. Robust Buyer mapping to facilitate implementation of auto-payment mode assignment and state-specific buying rules

8. Government to Government transactions that involved participation of private entity in the procurement process, on the Seller/ Service Provider side, to not be exempted from transaction charges and Annual Milestone charges. For instance, in case ONGC holds a bid to procure specialized equipment and bid participants include CPSEs such as BHEL and private players such as Reliance, then the order, even if won by a CPSE, will not be excluded from the transaction charges and Annual Milestone charges. However, in case there was no private entity participating in this bid, the order would be excluded *(currently ongoing)*

8.1.10 Incident Management

GeM is a trust-based system. As self-declaration is the key, strong automated processes to penalize any deviant behavior at GeM platform is a must. For this purpose, any action that is at variation from the terms and conditions of procurement on GeM and relevant Government rules and guidelines is termed as "deviation".

Incident Management Policy shall guide the on-line mechanism for reporting and initiating action on any such deviation and elaborates the overall framework for identification and handling of deviations on GeM portal.

Any of the below parties can raise an incident:

1. Buyer (all stakeholders including primary Buyer, consignee, PAO/ DDO, etc.)

2. Seller/Service Provider

3. GeM Admin

4. GeM portal (rule-based creation of incidents for specific reasons such as decline of Direct Purchase / L1 order, expiration of delivery period, etc.; in case of creation of incident by GeM portal, the same procedure as indicated in the policy would be applicable)

Buyer / Seller / Service Provider can create an incident on the Incident Management (IM) Dashboard and try to get a resolution mutually within the stipulated time from the party against whom the incident has been raised. In case of no resolution at user end, the incident can be escalated to GeM Admin after completion of the stipulated time. GeM Admin takes suitable action based on available facts and merit of the case. Proper anonymity is maintained by masking identifying details pertaining to Buyer and Seller/ Service Provider from GeM Admin and other internal users to ensure fair decision making.

As per the Incident Management Policy, no penalty shall be imposed for the same reason under the same Contract more than once, except for non-delivery related incidents which are allowed lot-wise in case of staggered delivery schedules. Similarly, in case of Services, more than one incident can be created, and penalty can be imposed for same reason of the contract with different duration.

8.1.10.1   Pre-contract:

Pre-contract phase involves Buyer/ Seller/ Service Provider/ GeM Admin raising an incident in case of reasons defined in the Incident Management Policy. Some of the reasons are wrong listing of product/ service, offering discontinues or end of life products, unreasonable offer price, misrepresentation of brand name/ brand category, wrong reporting of pre-contract incidents, etc. The detailed list of reasons can be found in the GeM Incident Management Policy and are subject to change as per policy revisions.

The following is the process flow for managing a pre-contract incident:
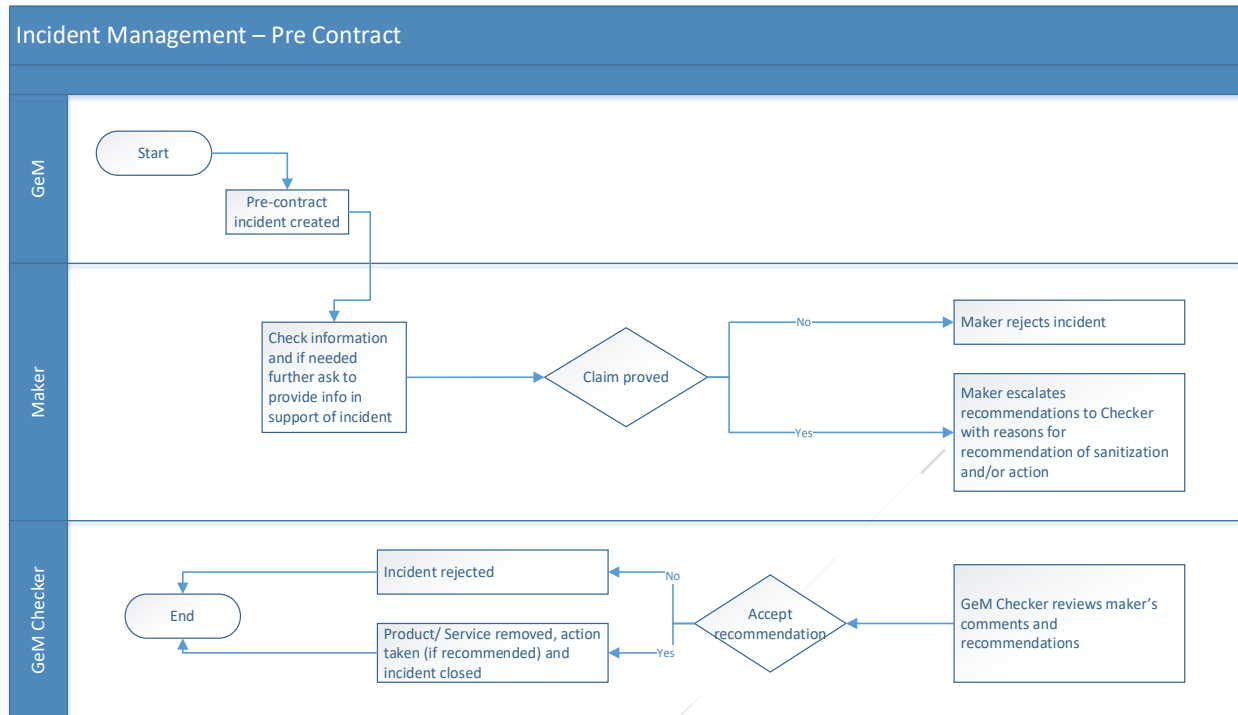
Figure 49: Pre-contract Incident Management

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Buyer/ Seller/ GeM Admin raises a pre-contract incident via Incident Management Dashboard	1.1	Dedicated incident management dashboard for users to raise and manage incidents (view status, discuss and mutually close incident with the other party, escalate incident, etc.)
		1.2	Users can also raise a pre-contract incident via product/ service page by clicking on 'Report this Product/ Service' button
2	Maker reviews the incident and validates the claim. If needed the maker can ask for further information for clarification		

3	If the claim is valid, the maker escalates recommendation to checker with reasons for recommendation of sanitization or sanitization as well as action against Seller/ Service Provider In case the claim is not valid, maker rejects the incident	3.1	Workflow to route request to Checker
4	GeM checker from incident team reviews maker's comments and recommendation		
5	If the recommendation is accepted, product/ service is removed, and wherever applicable, action is taken as per GeM's Incident Management Policy and incident is closed. In case it is not accepted, incident is rejected	5.1	Removal of product/ service from GeM portal

Table 78: Pre-contract Incident Management process and functionalities

8.1.10.2   Post-contract:

Post-contract incidents can be raised for deviations such as delay in delivery, delay in mobilization of services, non-delivery of product, non-compliance of SLA, violation of integrity pact, submission of fake documents, refusal to supply product/ services after placement of contract, etc. The detailed list of deviations/ reasons is provided within GeM's Incident Management Policy.

The following is the process flow for managing a post-contract incident:
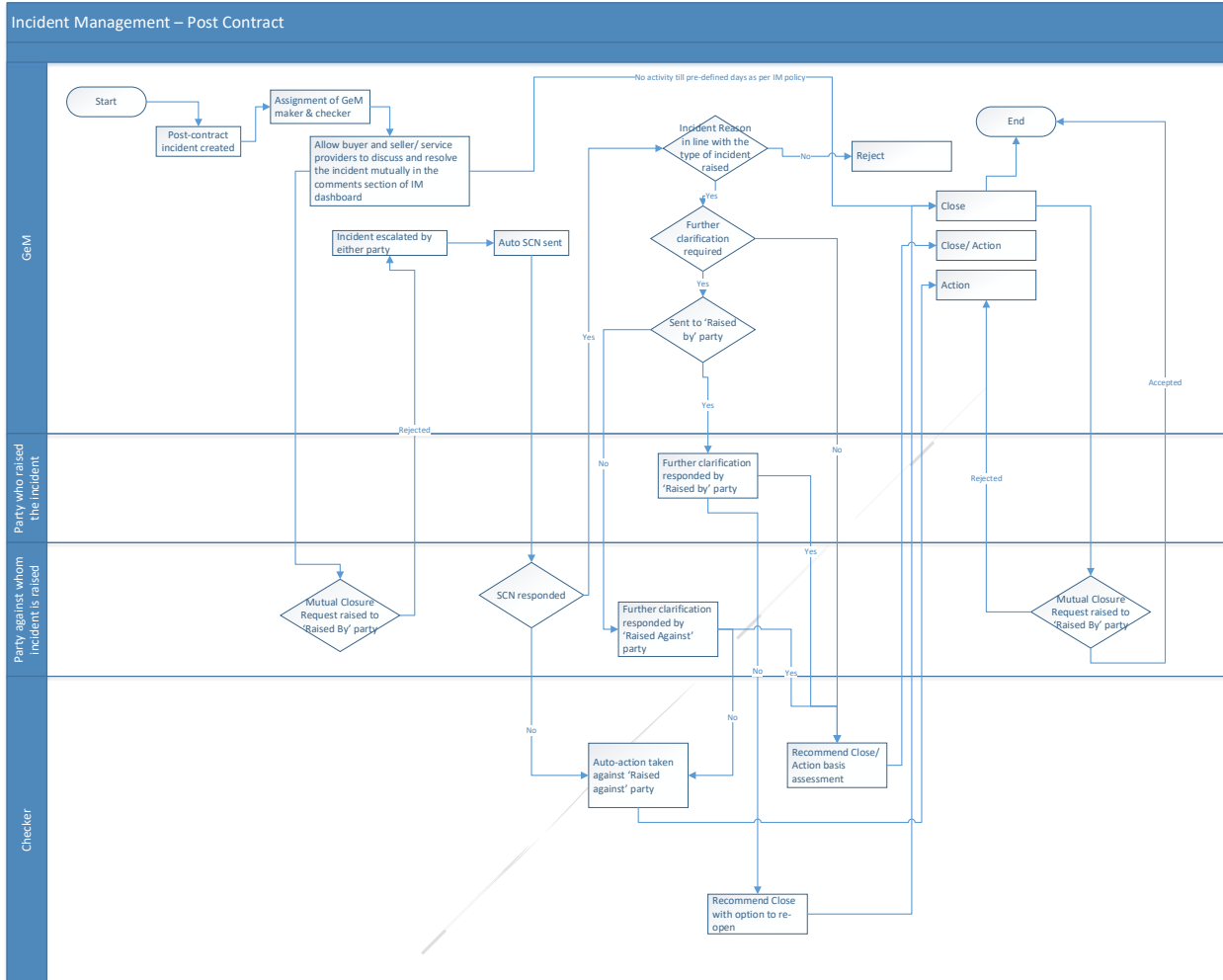
Figure 50: Post-contract Incident Management

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Post-contract incident is created by Buyer/ Seller/ Service Provider/ GeM admin/ GeM portal. In case the incident is created by a Buyer, the Buyer is asked to attach a debarment order (optional)	1.1	Dedicated Incident Management Dashboard for users to raise and manage incidents (view status, discuss and mutually close incident with the other party, escalate incident, etc.)
2	The incident is assigned a Maker who reviews the incident and related documents as well as a Checker who recommends action/ closure basis the data available	2.1	Sequential allocation of incidents to random Makers and Checkers within GeM
3	Once the incident is created, the involved parties (raised by and raised against) have the option to discuss and resolve the incident mutually in the comments section of IM dashboard. In case the incident is mutually resolved, 'Raised Against' party can send a 'mutual closure' request. If 'Raised by' party accepts the request, the incident is closed	3.1	Masked identities of 'raised by' and 'raised against' parties
		3.2	Dedicated comments section for discussion and mutual closure of incident as per guidelines in GeM Incident Policy
		3.3	Mutual closure option
4	In case the incident does not get resolved, either party can escalate it to GeM. Once the incident is escalated, a 'Show Cause Notice (SCN)' request is sent to the 'raised against' party. In case the incident reason is not in line with the category of incident raised then the Checker can 'Reject' the incident	4.1	Option to escalate incident to GeM
		4.2	Reject incident option
5	Raised against party responds to SCN within a stipulated time frame. Maker reviews the response and asks for further clarification from either party involved if needed. In case the raised against party does not respond to SCN despite warning, auto-action is taken against the party (as per debarment order attached; if debarment order is not attached by the Buyer, then as per GeM Incident Management Policy)	5.1	Option to Maker to send request for further clarification
6	Post this, the response for further clarification is	6.1	Auto-action basis codified

	received and reviewed, Checker either recommends action or recommends to close the incident. In case further clarification request was raised to 'Raised By' party and the party fails to respond within stipulated timelines, the incident is closed and can be re-opened at a later stage. In case further clarification request was raised to 'Raised Against' party and the party fails to respond within stipulated timelines, then auto-action is taken against the 'Raised Against' party as per debarment order/ GeM IM policy.		penalties as per GeM's Incident Management Policy, upon selection of 'action' option
7	In case further clarification is not required, recommendation is made by the Checker (action/ close) basis the information available, which is then implemented by the system. In case of an action, system automatically suspends 'Raised Against' party as per debarment order attached or GeM IM Policy (as applicable)	7.1	Automated action and system rules pertaining to action to be taken
8	'Raised Against' party can raise a mutual closure request even after the action has been taken. In case the 'Raised by' party accepts the request, incident will be closed, and all the impact related to that incident will be removed.	8.1	Discontinuation of action taken basis rules pertaining to mutual closure of incident

Table 79: Post-contract Incident Management process and functionalities

Once the incident is resolved, the parties involved also have a facility to submit an appeal (as per the process laid out in the Incident Management Policy) within a defined period of time post-resolution in case they are not satisfied with the resolution.

Provision of APPEAL

1. The option of APPEAL can be availed by Seller/Service Provider after imposition of penalty

2. The option of APPEAL can be availed only if there is any additional material evidence which was not available for consideration at the time of taking a decision by the Competent Authority of GeM.

3. Request for APPEAL can be made in 10 calendar days of imposition of penalty.

4. Provision of APPEAL is available only once against one incident for Seller/ Service Provider.

5. Further clarifications may be sought from Buyer/Seller/SP by GeM Admin, if required.

6. In case of receipt of satisfactory or unsatisfactory response, further action based on the facts and merits of the case and as per provisions of the IM policy will be taken by GeM Admin for either closure of incident or continuation of the penalty. In case of no response from the Buyer/Seller/Service Provider to the APPEAL or the clarifications sought, in 5 calendar days at each level, GeM Admin may take action based on available responses without giving any further opportunity or waiting for response.

7. The status of Seller/SP will not change during the period of consideration of APPEAL.

8. 5% of contract value with a minimum of Rs. 1000 and a maximum of Rs. 10,000 would be charged as fee for consideration of Appeal. In case the deviation is not linked to a specific contract, a fee of Rs. 1000 shall be charged for consideration of Appeal.

9. In case of decision in favour of Seller/Service Provider who applied for Appeal, the fee charged would be returned.

8.1.10.3   Additional interventions/ functionalities needed:

1. Process and policy related modifications/ enhancements to improve the process further and make it more efficient. This is an ongoing process with modifications being introduced periodically basis requirements arising as GeM evolves. Some modifications/ additions planned include *(currently ongoing)*:

    a. Introduction of Turn Around Time (TAT) at every critical stage of the process

    b. Auto-action in case of no response to SCN

    c. Auto-action in case of no response to further clarification by raised against party

    d. Auto close with option to re-open incidents in case of no response to further clarification by raise by parties, etc.

    e. Senior GeM stakeholders to act as Checker w.r.t pre-contract incident management process

2. Forward Auction related reasons (e.g., non-compliance by H1 bidder, etc.) to be included in the Incident Management Policy

3. Implementation of online appeal process post payment integration *(currently ongoing)*

4. Mutual closure option to made available to parties involved post SCN is sent *(currently ongoing)*

5. Option to create incident against Seller/Buyer to be provided to tackle issues where there are no order/bid/catalogue available.

6. System related changes such as optimization of Incident Management Dashboard to improve user experience and interface, auto-closure of incidents based on change in system status (e.g., CRAC not generated incident auto-closed in case CRAC is generated by the Buyer), mandated fields to upload documentary evidence basis incident reason, etc.

7. User-friendly Incident Management Dashboard to be created for GeM admins and other users (Buyers, Sellers, Service Providers, etc.) to work on incidents and monitor pendency, TAT, etc. Further, automated reports on key metrics shall be sent by MSP to GeM as per alignment with GeM

8. Appeal dashboards to be provided at ACEO level. Appeal related automated reports to be sent to GeM officials on timely basis

9. System generated incident creation to be enabled based on rules defined by GeM in alignment with the Incident Management Policy

10. Analytics based decision support system shall be developed to equip the evaluating officer with all the relevant details (e.g., past default history of party against which incident has been raised, past suspensions, etc.) while evaluating incidents to facilitate decision making

11. Automated processes to be implemented to make system smart enough to detect if cause of incident is resolved and take action/close incident accordingly (e.g., In case an incident was raised because the CRAC against an order was not generated, the system should be able to automatically detect if the CRAC has been generated and close the incident)

8.1.11 Request Management System

Request Management System can be used by various stakeholders to raise the following requests:

1. Procedural or policy request

2. Category updation (for Buyers, Sellers, and Service Providers)

3. New category creation request (currently under revamp)

Procedural or policy request (only for Defence HoDs)
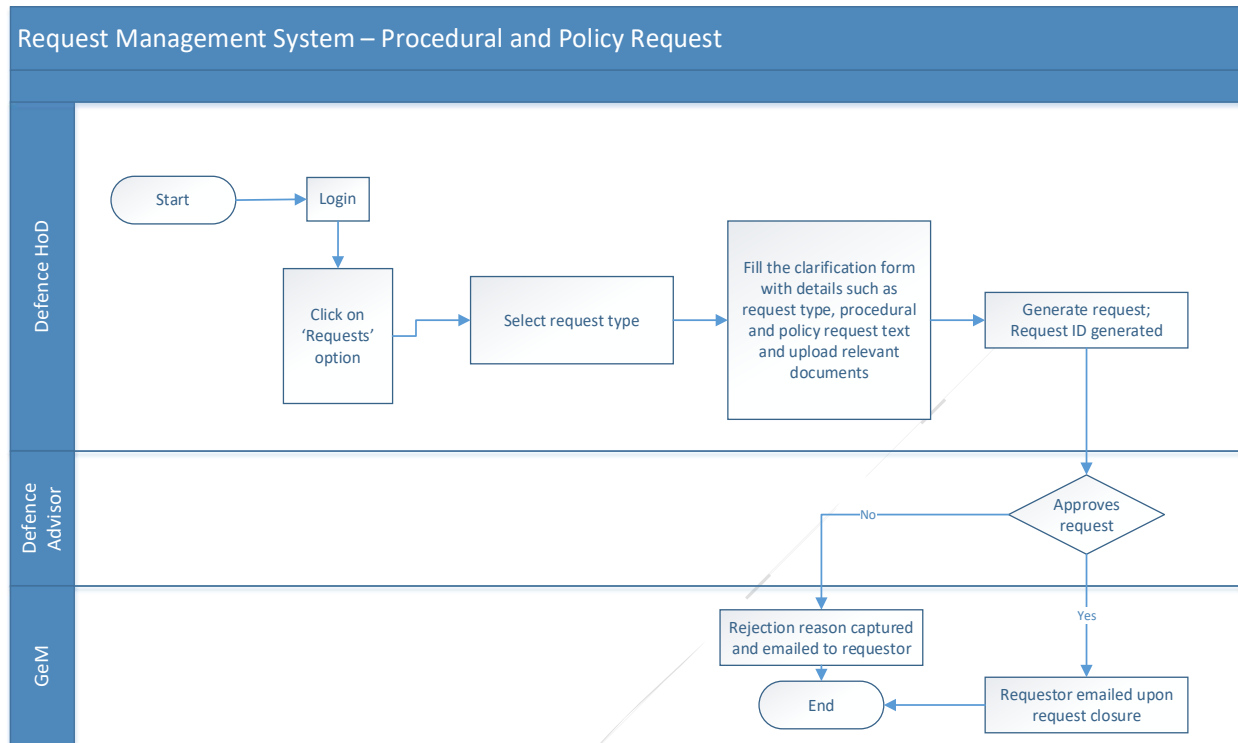
Figure 51: Procedural or policy request

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	The Defence HODs will get an "Requests" option on his dashboard for raising a clarification request		
2	The HODs would select the "Procedural or Policy Request" option from the Request Type drop down on the Request Management Screen to submit a new clarification request		
3	The HOD will get Clarification form with following fields:	3.1	Document upload and storage functionality (on cloud)

	1. Request type: Procedural or Policy Request 2. Procedural or Policy Request text 3. Upload Document: HODs can upload any document for this request. Document type supported by the system should be doc/pdf/excel. The max size of upload is 5 MB.		
4	The user will click on the "Generate Request" button after providing the mandatory information. In case of any discrepancy, the system will display an error to provide the mandatory information. After passing the validation, the user will be displayed the Request ID number generated against the raised request. The HOD can track the request using the request ID respectively. The status of the request will be set to "Under Consideration"	4.1	Request generation and request ID creation
5	The Procedural or Policy Request verification would be done by Defence Advisor. The RMS request will be provided to the Defence Advisor admin ID if it already exists, else a new Admin ID is created, and RMS access will be provided to that ID. The Defence Advisor would receive the Procedural or Policy Request from the Defence HoDs. The Defence Advisor will take the required action against the request under this section.	5.1	Automated routing of request to Defence advisor for resolution
		5.2	A confirmation email gets triggered to Defence HOD upon closure of request and the request gets closed

Table 80: Procedural or policy request process and functionalities

Category updation (for Buyers, Sellers and Service Providers)

Buyer or Seller/ Service provider can raise category updation/ modification request to GeM. The following section details out the process further:
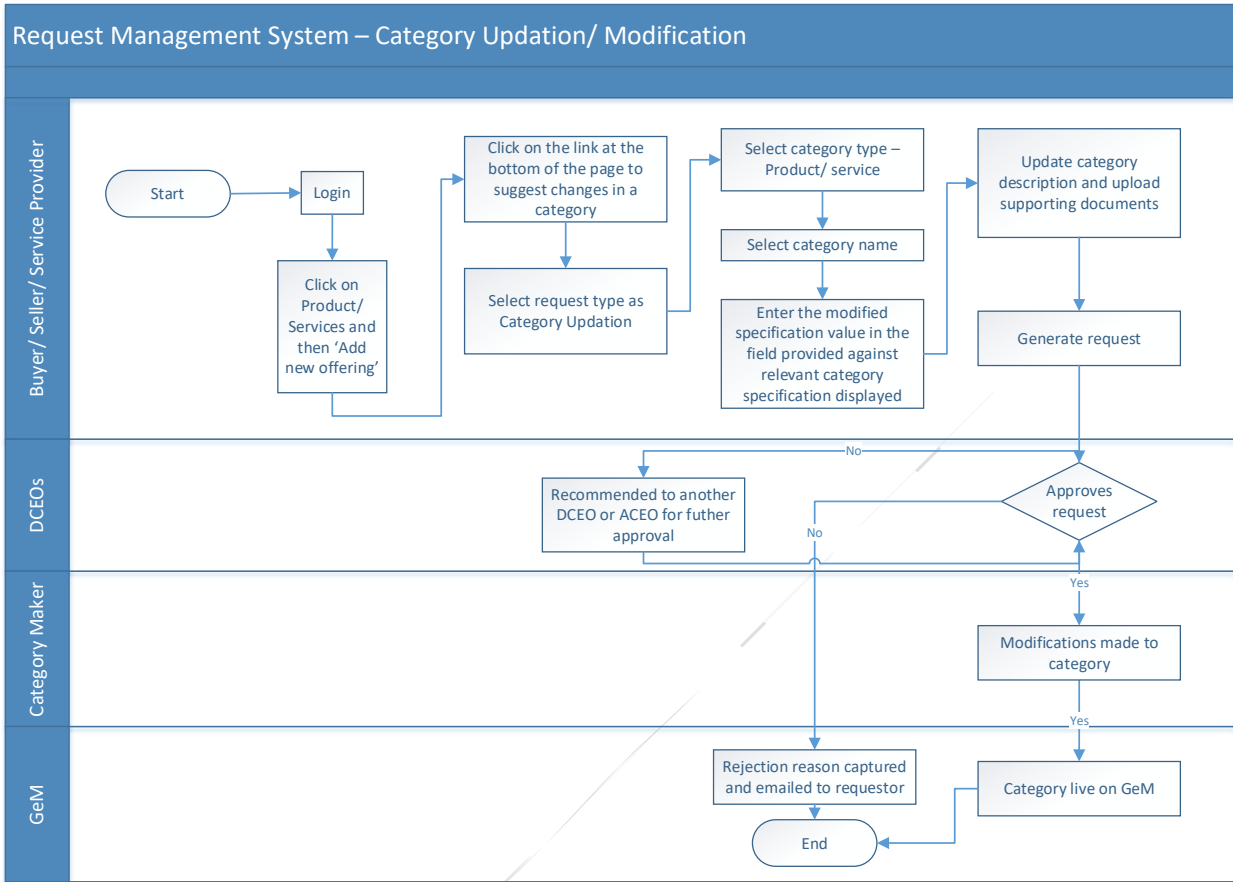
Figure 52: Category Updation/ Modification Request

Detailed Process Flows			
#	**Process Steps**	#	**System Functionality**
1	Buyer/ Seller/ Service Provider logs in and clicks on 'Product'/ 'Service' and 'Add new offering'		
2	Buyer/ Seller/ Service Provider clicks the new category creation link in the bottom of the page to submit a request to add a new category		
3	Buyer/ Seller/ Service Provider selects the		

	request type and selects the request for category upgradation		
4	Buyer/ Seller/ Service Provider selects either product or service as category type, and selects category name	4.1	Category name and type mapping
5	After this, Buyer/ Seller/ Service Provider submits their specific change request by entering the proposed value against the respective specification	5.1	Category specification list visible basis category selected
6	Following this Buyer/ Seller/ Service Provider submits the updated category description and uploads supporting documents and clicks on 'Generate request'	6.1	Document upload and storage functionality (on cloud)
7	The DCEOs of the requested Category would receive the request from the Buyers/Sellers/Service Providers and evaluate the request. The DCEO would recommend the request with additional comments for changing the specifications and can either approve it, reject it or assign it to ACEOs for further approval. After approval, the modifications are made in the system. In case of rejection, the rejection reason is captured and notified to the requestor	7.1	Email will be sent to Buyers/Sellers/Service Providers with rejection reason and same will be shown on the Buyers/Sellers/Service Providers Dashboard
		7.2	Dashboard for DCEO/ACEO to have visibility on requests that have been rejected, recommended, and approve
		7.3	Admin Access for Requests: The DCEO/Shopclues will be able to view the logged request in a dashboard in the admin panel (assigned privileges)

<p align="center">**Table 81: Category Upgradation process and functionalities**</p>

New Category creation (for Buyers)

Buyer can raise new category creation request to GeM. The following section details out the process further (process is currently being implemented):
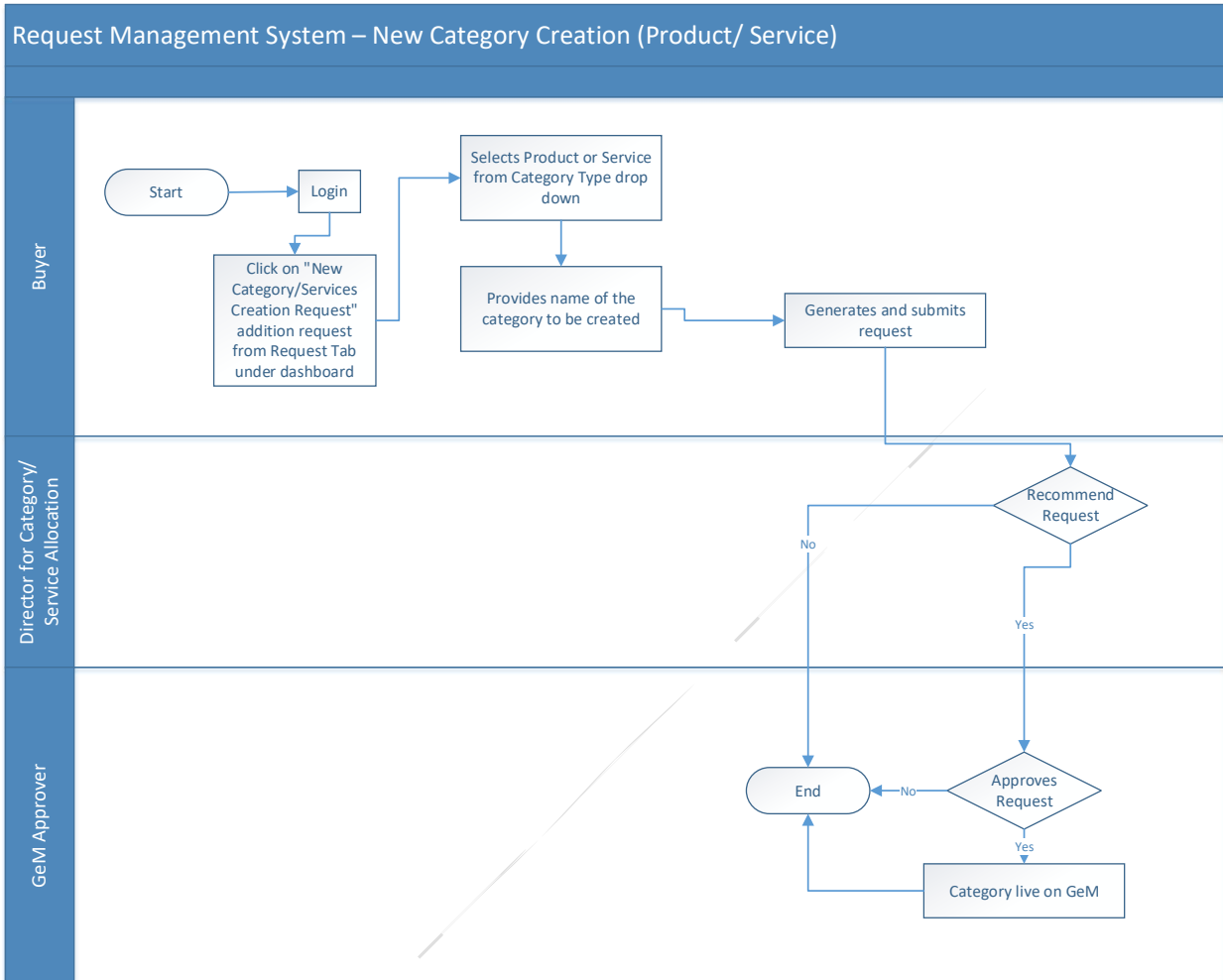
Figure 53: New Category Creation Request

Detailed Process Flows			
#	**Process Steps**	**#**	**System Functionality**
1	Buyer user will initiate the "New Category/Services Creation Request" addition request from Request Tab under dashboard		
2	Buyer selects the request type as New Category/Services Creation Request and	2.1	Dropdown list with relevant option to

	selects Product/ Service from category type drop down		select
3	Buyer provides the name of the new category to be created	3.1	"New Category/Service Name" textbox
4	After submitting the request, the logged request will be sent to "Director for Category/Service Allocation",	4.1	User role with appropriate privileges and RMS dashboard to manage requests
5	The Director for Category/ Service Allocation can Reject or Recommend the request. In case Director for Category/Service Allocation recommends then the approver will have the access to approve/reject the request. In case Request is rejected by Director for Category/Service Allocation then the request process is stopped, and status is updated and shown to the Buyer under view Request Type section	5.1	RMS dashboard with proper workflows and status flags to manage requests

Table 82: New Category Creation process and functionalities

8.1.11.1 Additional interventions/ functionalities needed:

1. System to be made agile with a dashboard at all the levels at GeM for any future requirement where Buyer/Seller can raise request (e.g., request for Additional Terms & Conditions, feature update/ enhancement request, etc.), and the same can come to GeM(maker-checker) for approval and automated action. Dashboard for each user (e.g., Buyer, Seller, GeM-Maker, GeM-Checker, etc.) to be provided and automated reports for GeM officials to be provided for tracking TAT and pendency

8.1.12 Learning Management System

LMS is a tool/platform to cater to the training needs of individual stakeholders of GeM be it Buyers, Sellers, or trainers. The platform has complete repository of GeM's training material, FAQs, Feedback for training, Attendance etc. GeM LMS is an invaluable, user-centric knowledge repository featuring learning paths to meet user specific needs and learn the ecosystem better. It serves as a platform for users and trainers facilitating intermediate processes like registration training, live training using webinar, certification, feedback, FAQs, and other user specific journeys. Some key features of LMS include:

1. Asset Repository

2. Micro Learning

3. User Journeys

4. Social Media Feeds

5. Certification

6. Learning Ecosystem

A Buyer or Seller registered on GeM can use his/her credentials to log in to the LMS. Training institutes can also be a part of the LMS portal after their ID and passwords are created, post a request for account creation is raised to GeM. Once logged in the user has access to all the material available on the LMS portal.

Apart from LMS, GeM also offers offline trainings at the request of organizations via trainers (MSP team). Additionally, GeM also has dedicated business facilitators for states that help the Buyers to get familiar with the GeM portal and aid the users in case they are facing any issue w.r.t using the GeM portal.

8.1.12.1 Additional interventions/ functionalities needed:

1. Tracking of time spent by user on LMS
2. Fully functional and updated, multi-lingual LMS portal with engaging certification tests
3. Fully functional, multi-lingual demo portal purpose (updated monthly to reflect all latest changes in the platform) for training to allow users to practically experience GeM portal
4. Vernacular availability of training material on LMS and for certifications
5. Calendar for State training visible on LMS

8.1.13 Inspection and Quality Testing through Empaneled Agencies

While creating a product bid, an option is available to the Buyers to avail Inspection for the products being procured via the bid. This is non-mandatory & selected as 'No' by default. If a Buyer selects 'Yes' w.r.t 'Is Inspection Required', the system will ask them to select their 'Empaneled Agency/ Inspection Authority' (e.g., DGQA, DRDO, EIL, NITRA, etc.) that will be conducting the inspection to ensure that the product conforms to the contractual requirements.

If the Buyer selects 'Yes' w.r.t 'Is Inspection Required', Buyer has to follow the below steps to avail inspection while creating product bid:

1. Buyer has to choose the "Type of Inspection" and the same will be printed on the Bid document

   a. Pre-dispatch / Stage wise Inspection which happens at Seller Premises before product dispatch and the Seller must mention "Place of Inspection, Contact Person Name & Contact number" while participating in the Bid

   b. Post-dispatch Inspection which happens at the consignee location before acceptance of the product by consignee

2. Buyer has an option to attach the 'Quality Assurance Plan' document in PDF format, but this is optional

3. Buyer has to choose inspection clause from ATC

4. Once the Bid is awarded, the Buyer must mention the name of the inspecting officer corresponding to the inspection authority/Agency selected during the bidding stage

5. All these details 'Type of Inspection, Name of Inspection Agency/ Authority, Name of the Inspecting officer & Place of Inspection' will be displayed on the contract document

6. An email will be sent to the inspecting officer mail ID informing about the Bid and Seller details

8.1.13.1 Additional interventions/ functionalities needed:

1. Functionality to onboard Inspecting Authorities and inspectors (via creation of dedicated user roles for inspection agencies, integration, etc.) on GeM and enable them to upload inspection reports, certificates, etc., which shall be accessible to relevant (internal and external) stakeholders. There should also be an inspection related dashboard, accessible to relevant users, with details around inspection requests raised, status of request, report against each request, etc.

2. Functionality to enable Buyers who do not have empaneled inspection agencies, to procure the inspection services by selecting an inspection/testing agency via GeM

8.1.14 Audit Trail

An Audit Trail is a step-by-step record of any action or transaction performed in the system. An audit trail is important because it is used to verify and validate business transactions by tracking selected user activities, event source, and data access used to create or modify a record.

A robust audit trail needs to be developed, which includes capture of step-by-step record of all actions and transactions related to all processes at GeM with time stamp. For instance, audit trail should capture actions related to procurement processes such as bid tables, shopping cart process, historical prices during negotiations with Sellers/ Service Provider, finance related trails, actions pertaining to request management system, etc. The decision/ data points to be captured as part of audit trail, along with access privileges (e.g., audit trail to be accessible to all above in hierarchy, audit team, vigilance team, etc.), etc. will be finalized by GeM.

Audit Trail will also have a screen capture functionality, with proper workflow to provide specific users access to the screen recordings with proper approval process.

MSP shall also develop a functionality/dashboard where GeM authorized users can check the audit trail data at any point of time without routing the request for the same through MSP.

Audit Logs shall remain only for view purposes.

Products:

Indicatively, an update of bid module audit trail is needed to capture all the touchpoints related to the bid module, e.g.:

1. Buyer details and action performed during bid submission

2. Seller details and action performed during participation

Similar to the bid module, there should be an audit trail for Sellers, Buyers, CMS, fulfillment, admin, payment modules so that complete information can be retrieved as and when needed.

Services:

In case of services, the audit trail must capture the following (indicative list):

CMS:

1. Every action performed by the user within the system must be recorded

2. Creation of Service details with the time stamp

3. Every update /change within the service to be recorded with the approving authority details and the time stamp

4. Admin/authorized person must have the right to view the action performed within specific category and the no. of iterations performed

Third Party verification: Admin shall have option to view the action performed by the third party during the verification process

Service Provider: Every action of the Service Provider must be recorded within the system. Service provider details starting from profile change/update, category visited, price changes, category update, certificate change, RA participation, negotiation, price match, bid participation, documents uploaded by the Service Provider must be recorded with the user type (Primary/secondary user). Service Provider participation details and invoices raised must also be captured with the timestamp.

HoD:

1. HoD of the Buyer organization must have right to view all the action performed by Primary Buyer, consignee, payment authority, and all other secondary user roles created in the future

2. Timestamp must be recorded with every action

3. HOD must be able to view the contract details, no. of Service Providers participated, documents uploaded by Service Provider, documents uploaded by Buyer, payment details, SDAC document, supporting document uploaded by Service Provider, Tax invoice, approvals uploaded in Bids/contracts, draft bid creation

8.1.15 Vendor Rating Assessment

Currently the vendor rating assessment is only done in case of products. An objective methodology has been deployed to calculate Seller rating on GeM using varying weightages for different variables, namely delivery, reliability, quality, users' feedback, and Buyers' feedback. Additionally, the rating calculated is adjusted based on the penalty arising out of reporting of incidents, i.e., the Seller's non-compliance with the terms and conditions agreed between the Seller, Buyer, and the GeM platform. Methodology will be provided by GeM and MSP shall provision for system-based automated calculation of vendor rating and periodic updates to the same across all Sellers on GeM.

8.1.15.1 Additional interventions/ functionalities needed:

1. A robust rating framework also needs to be introduced for Service Providers and Service Provider rating must be displayed on GeM *(currently ongoing)*

8.1.16 Advanced Analytics and Business Intelligence

BI GeM dashboard is an information management tool that visually tracks, analyzes and displays key performance indicators (KPI), metrics and key data points to monitor the overall business process. Various stakeholders such as Ministries, State, Cabinet Secretaries (Cabsec), HOD, Buyers and Nodal Officers associated with GeM can easily analyze their respective data with these Analytics Dashboards. Below dashboards are available for various internal and external users in the form of user access enabled dashboards or automatically generated, periodic reports.

MSP shall be responsible to develop and maintain the below mentioned dashboards and reports. The final list of reports/ dashboards to be created, their refresh/ publication frequency (will vary across dashboard and reports), and user access related details shall be aligned with GeM during the design phase as mentioned in Volume 1 Section 5 of this RFP.

Name	Type (Dashboard/ Report)	User type
Ministry View	Dashboard	External
State View	Dashboard	External
Ministry & State View combined	Dashboard	External
CPSE Dashboard	Dashboard	External
Cabsec View Dashboard	Dashboard	External
Category Owners Dashboard	Dashboard	Internal
Nodal Officer Dashboard	Dashboard	Internal
ACEO View	Dashboard	Internal
CEO View	Dashboard	Internal
GeM MSP	Dashboard	Internal
GeM Utilization Ratio (GUR) Dashboard	Dashboard	Internal
Anomaly Dashboard	Dashboard	Internal
Incident Management (IM) Dashboard	Dashboard	External and Internal
IM – CEO	Dashboard	Internal
IM Productivity Dashboard	Dashboard	Internal
Buyer Dashboard (implementation ongoing)	Dashboard	External
Business Cockpit	Dashboard	External

CGDA Dashboard	Dashboard	External
Price Trends	Report	External
Vendor Assessment	Dashboard	Internal
GeM Control Tower	Dashboard	Internal
BIDS Cancellation	report	
GeM Transactions Dashboard 3.0	Dashboard	External and internal
SHG Dashboard	Dashboard	External
Payment Invoice Dashboard	Dashboard	External and internal
Product Dashboard	Dashboard	Internal
Brand Dashboard	Dashboard	Internal
ReB Dashboard	Dashboard	External
MRP Change and Catalogue Summary Dashboard	Dashboard	Internal
Seller KPIs	Dashboard	
CRM Dashboard	Dashboard	Internal
Notification Matrix		Internal
Operational Reports	Reports	Internal
Brand Processing	Report	Internal
Product Pendency Report	Report	Internal
Cancel By Seller Orders Report (Ministry of Railways)	Report	External
CRM Reports	Report	Internal
Sub-category Purchase Price	Report	Internal
Seller Assessment Summary	Report	Internal
Payment Due Report	Report	Internal
Offline Payments Report	Report	Internal
Ministry, State and CPSU Payment Due	Report	Internal
Buyer Ageing Payment Stats	Report	Internal
Transaction Charges Report with Annual Milestone Charges	Report	Internal
Daily Seller, OEM and product addition Report	Report	Internal
Daily Transaction Volume	Report	Internal
Admin System Stats	Report	Internal

System Transaction Trends	Report	Internal
Category Wise Transaction Status	Report	Internal
Location Wise Transaction Status	Report	Internal
GeM Transactions Overall Report	Report	Internal
Seller Active Orders Summary	Report	Internal
Seller Rating	Report	Internal
Seller Summary Report	Report	Internal
GeM DDR	Report	Internal
Fortnight Report	Report	External and Internal
BoQ Bids Report	Report	Internal
Ongoing Ministry bids with estimated value more than 5 Cr	Report	External and Internal
Services Flag Report	Report	Internal
Daily Sales report	Report	Internal
Weekly report for services	Report	Internal
GeM Monthly Report	Report	External and Internal

Table 83: Dashboards and Reports

The dashboards created by MSP shall be audited by third party agency (CERTIN empaneled) to ensure data integrity/ cyber security/ authenticity etc.

MSP shall also provision for enterprise level licenses of software approved by GeM so that no. of users with access does not become a restriction during the duration of this contract.

Apart from dashboard and reports, MSP shall also implement Advanced Analytics/ AI/ ML related use cases as aligned with GeM during design phase – e.g. procurement planning, product recommendations, product demand forecasting, etc. In addition to this, MSP shall be responsible for implementation of existing use cases currently implemented/ being implemented by GeM or third-party nominated by GeM such as market intelligence gathering (competitive analysis, price benchmarking), duplicate image identification to ensure catalogue accuracy, identification of anomalous behaviour (collusion, cartelization, etc.), bidding analytics (measure health of a bid by assessing participation, Seller offering, L1 price) and NLP based search engine.

Additional interventions/ functionalities needed:

1. Creation of additional dashboards/ reports as aligned with GeM during the design phase as mentioned in Volume 1 Section 5 of this RFP without additional costs . For example:

    a. Services Dashboard (including no. of Bids/ orders created within a particular service, no. of Service Providers registered under the category, no. of successfully executed

orders, etc.)

b. HR Dashboard

c. Legal Dashboard

d. Custom reports on key metrics for key Buyers/ Sellers, as aligned with GeM

e. Reports for internal system auditor, IT security, etc.

f. Category Brands OEM details (including category ID, category name, brand name, brand OEM name and brand OEM TM document)

g. Category reseller details (including category ID, category name, brand name, reseller name)

h. Category statistics report (including category ID, no. of catalogues, no. of total bids, no. of active bids, total BID value, no. of total orders, total order value, etc.)

i. Seller reporting on dynamic filters like GSTN, Business PAN, Caution money, MSE, Startup etc.

j. Category reporting on dynamic filters on category configurations (Quadrant, OEM count, various flags)

k. Brand application status report (including category, brand type (registered, unregistered, etc.), trademark /document was used for brand creation, application status (approved, rejected, etc.), brand status (active, inactive, etc.)

l. Inspection Dashboard (including details around inspection requests raised, inspecting agency, inspection status, inspection details, etc.)

m. Custom reports for services (e.g., prices for packages with different combination of services, etc.)

n. Monthly reporting on new feature introduced to GeM (to be published on GeM platform)

2. Enhancement and refinements in current dashboards/ reporting structures, as aligned with GeM (e.g., Incident Management Dashboard should be revamped to offer visibility on pendency, TAT, etc.; Seller dashboard must have category wise, ministry/state/department wise, OEM/Reseller business wise, Seller business (Direct Purchase /L1/BID/RA), VA/VAE

views, etc.)

3. Expanding user access for dashboards/ reports as required, and improvement/ refinement of current dashboards/ reports to cater to different users

4. Implementation of existing and new AI/ ML related use cases/ interventions/functionalities as aligned with GeM during design phase – e.g. NLP based search engine, market intelligence gathering (competitive analysis, price benchmarking), duplicate image identification to ensure catalogue accuracy, identification of anomalous behaviour (collusion, cartelization, etc.) bidding analytics (measure health of a bid by assessing participation, Seller offering, L1 price), procurement planning, product recommendations, product demand forecasting, etc. *(currently ongoing)*

5. Personal Identifiable Information must be masked in the dashboards and reports wherever applicable

8.1.17 Administration

The Administration team is responsible for creating internal/ external user roles with specific responsibilities and privileges to support the processes on GeM. While this is currently done via a back-end process, MSP shall setup a module with admin user defined for creation / deletion / management of different roles / profiles in alignment with GeM. The following is a list of user roles currently supported by the GeM system along with a role description.

S.No.	Role Name	Detailed description
1	ACEO	To manage all ACEO tasks from admin panel: 1. Category Tag Mapping 2. CMS 3. CMS Dashboard 4. CMS Services 5. Dashboard 6. Forum 7. Incident Management 8. Manage Workgroups 9. Market Management 10. Marketplace 11. NULL

		12. OEM Dashboard
		13. Order
		14. Order List
		15. Orders Management
		16. Portal Management
		17. Product
		18. Product Management
		19. Request Management
		20. Terms And Conditions
2	ADVISOR	Advisor will have access to :
		1. Incident Post Contract
		2. IM Dashboard
		3. LMS Report
3	AIR TICKETING	To view Air Ticketing details through Admin Panel by GeM
4	ANALYST	To analyse data on GeM:
		1. Analytics Reports
		2. IM Dashboard
		3. Order
		4. Predictive
		5. Real Time
		6. Reports
5	ATC APPROVER	RMS access to approve Additional Terms and Conditions (ATC) through Admin panel
6	ATC RECOMMENDER	RMS access to perform actions such as recommending appropriate action for request
7	ATC-APPROVER	RMS access to approve RMS requests from dashboard
8	ATC-LEGAL	RMS access to perform legal action
9	BID AUDIT VIEW	To view BID related information on Admin dashboard:
		1. Audit Trail

		2. Bid/RA
		3. Bid/RA View
		4. Direct/L1 Purchase
10	BID CORRIGENDUM UPLOAD	To upload BID corrigendum on portal by MSP
11	BID L1 NEGOTIATION	To perform L1 negotiation in Bid
12	BID VALIDITY EXTENSION	To extend Bid Validity
13	BIDDYNAMICREPORTS	To view Bid related reports (View Only).
14	BIS	Allows users to upload BIS data
15	BUDGET UNBLOCK	To enable user to unblock funds
16	BULK EMAIL TASK	To perform Bulk Email task
17	CAUTION MONEY	Access to caution money related information
18	CGDA-ADMIN	Access to CDGA related information
19	CMS SERVICE	To view and manage CMS services
20	CMS USERS	To enable access to CMS user details
21	COCKPIT FEEDBACK	To view feedback on Business Cockpit
22	CPPP REPORTING	Access to CPPP reporting view
23	CPPP TENDER ANALYSIS	To view CPPP Tender analysis
24	DCEO	Access given to DCEOs to view all activities from admin panel
25	EXTENDRA	GeM User will be able to view: Bid Management Ra Extension
26	FINANCE	Access related to Financial analysis and reporting
27	FINANCEKPI	To view Finance KPI
28	GeMBUYERIDREQUESTS	View GeM Buyer requests on admin panel
29	Helpdesk Admin	To enable Helpdesk to view below details related to support: 1. Dashboard 2. GeM 2.0

		3. Incident Management 4. NULL 5. Order 6. Order List 7. Order Search 8. Orders Management 9. User Management
30	IM APPEAL APPROVER	To approve incidents from admin panel
31	IM DECODER	To perform task related to decoding IM IDs
32	IMADMIN	To manage all the incidents related activity
33	INCIDENT ACTION APPROVER	To approve incidents from admin panel
34	INCIDENT ACTION RECOMMENDER	To recommend and reassign incidents from admin panel
35	INCIDENT VIEWER	To view Incidents details
36	INSPECTION AGENCY RECOMMENDER	To recommend Inspection Agency for Buyer Organizations
37	JD	JD role to perform action in RMS module.
38	JOB POSTING	For HR to post career related posts on portal
39	LEGAL	Role created for legal related tasks
40	MARKETINGKPI	To view Marketing KPI
41	MIS Payment Admin	To view MIS payments related reports
42	MKP PORTAL	To access Marketplace portal through Admin Panel
43	MSP ADMIN	To enable MSP to access operational reports such as: 1. L1 Negotiation 2. Audit Trail 3. Bid Logs 4. Bid Management 5. Bid Notification

		6. Bid Validity Extension
		7. Bid/RA
		8. Cancelled Bids
		9. Enable MSE
		10. E-Sign
		11. Extended Bids
		12. Merge Consignee
		13. Open Bids
		14. Published Bids
		15. Upload Corrigendum
44	MSP OPS	Access to Forum, Consultative Committee Meeting and Market Management
45	MSP-BUSINESSOPS	To enable MSP to access Request Management
46	MSP-ITOPS	To enable MSP to access IT related operational reports
47	NODAL OFFICER	To enable Nodal Officers to check reports like CGDA, DEFENCE MIS, Payment
48	ORDERDETAILS	To view order details as below: 1. Order List 2. Order Search 3. Orders Management
49	ORG APPROVER	To view and approve organization assigned to nodal officer
50	Organization Admin	To view all organization requests and to map nodal officers to State/Ministry
51	PFMS-ADMIN	To access PFMS related information like Budget Unblock, CGDA, Code Head, Payment, PFMS etc.
52	PIIDATACCESS	To view PII Data of Buyer, Seller from Admin Portal
53	PORTAL MANAGEMENT	Role will have access to all the functionalities of Portal Management
54	PRODUCT ADMIN	To enable Product related information like Product Dashboard, Pre Contract, Incident

			Management to be viewed by Product Team members
55	PRODUCT ADMIN MANAGER		To enable Product admin access for managing products with options: Incident Management Product Manager
56	REQUEST MANAGeMENT		View request management requests with Request Management tab
57	RM DIRECTOR PRODUCT		RMS director can perform RMS defined actions for product
58	RM DIRECTOR SERVICE		RMS director can perform RMS defined actions for services
59	RM-ADMIN		To manage RM details from admin panel with below options: 1. Order List 2. Order Search 3. Orders Management 4. Request Management
60	RMS ADVISOR		To perform RMS actions related to advisor with below options: 1. Advisor Dashboard 2. Request Management
61	SELLER MANAGeMENT		For GeM Seller Management team to have access to : 1. CMS Services 2. Forum 3. Marketplace 4. OEM Dashboard 5. Portal Management
62	Social Media Admin		To manage all Social media tasks from admin panel by Marketing team like below: 1. Dashboard

		2. Events
		3. Forum
		4. Gallery
		5. Health Check
		6. Maintenance
		7. News
		8. Portal Management
		9. Press Release
		10. Scroll Ticker
		11. Testimonials
63	STARTUP INDIA	To view information related to startup India
64	Support	Functionality to access User query related information on admin portal directly as below: 1. Dashboard 2. Brand Approval 3. Buyers 4. Department 5. GeM Buyer ID 6. Helpdesk 7. Incident Management 8. Market Management 9. Ministry 10. Order List 11. Order Search 12. Orders Management 13. Organization 14. Payment 15. Pending Buyer Requests 16. Product Approval 17. Request Management 18. User Management 19. User Search

65	TICKER UPDATE	To update Scroll Ticker on portal directly from admin
66	TRAINING ADMIN	To manage training activity /resources directly from admin panel: 1. Add New Press Release 2. Events 3. FAQ 4. FAQ Data 5. Form Submission 6. Forum 7. LMS 8. LMS participation feedback 9. LMS USERS 10. Portal Management 11. Reports 12. Testimonials 13. Training Management 14. Training Nomination 15. Training Requests 16. Upload CCM 17. Upload Pdf/videos 18. User Management 19. User Search
67	UNWORKABLEL1	To enable Bid Management and Disqualify Unworkable L1
68	USER MANAGeMENT	To enable GeM User access, manage admin user IDs /CMS users/LMS user management: 1. Activity Log 2. Add Role 3. Add Users 4. Admin Console 5. Admin Users 6. Buyers

		7. Category Tag Mapping
		8. CMS
		9. CMS Dashboard
		10. Department
		11. Edit Users
		12. GeM Buyer ID
		13. LMS USERS
		14. Manage Workgroups
		15. Market Management
		16. Marketplace
		17. Ministry
		18. OEM Dashboard
		19. Organization
		20. Pending Buyer Requests
		21. Role List
		22. Sellers
		23. Sub User Lists
		24. User Management
		25. User Search
69	USER MANAGeMENT MSP	MSP to manage Users and other requests for CMS /LMS user management
		1. Activity Log
		2. Add Role
		3. Add Users
		4. Admin Console
		5. Admin Users
		6. Buyers
		7. CMS Users
		8. Department
		9. Edit Users
		10. GeM Buyer ID
		11. LMS USERS
		12. Ministry

			13. Organization
			14. Pending Buyer Requests
			15. Role List
			16. Sellers
			17. Sub User Lists
			18. User Management
			19. User Search
70	WORKGROUP MAPPING		Workgroup mapping can be done from Admin Panel with two tabs mapped as below: 1. Incident Management 2. Workgroup Mapping

Table 84: Admin User Roles

8.1.17.1   Additional interventions/ functionalities needed

1. Refinement of existing roles (merging roles, deletion of unused roles, etc.)

2. Creation of additional roles with configurable access rights and privileges in alignment with GeM (e.g., AMC role, Vigilance role (for Buyer/ GeM/ CVC users), Audit role (for GeM/ CAG), etc.)

3. Any interventions/ modifications currently implemented from the back-end (e.g., revoking cancellation of order via back-end, changing Seller details in case of Merger/ Acquisition/ Demerger, etc.) should be implementable via front-end utility for GeM Admins and stage reversal functionality for Sellers/ Buyers/ Service Providers and GeM Admins while maintaining complete audit trail

4. Platform content shall be managed via CMS module and admins with proper maker-checker process

8.1.18 External Integrations

Following is an indicative list of integrations that are live in current GeM platform. Final list of integrations for the Go-Live criteria shall be aligned with GeM before submission of detailed project plan as mentioned in Volume 1 Section 5 of this RFP.

1. Buyer: e.g.,

a. Ministry of Defence

b. Railway iMMS, iRePS *(currently ongoing)*, IPAS integration

c. CRPF Integration

d. CGDA Integration

e. Ministry of Panchayati Raj integration (e-GramSWARAJ)

2. Third parties:

a. Payment integrations: e.g.,

i. Banks

- GeM Pool Account integration

- Online EMD integration with multiple banks *(currently ongoing)*

- BG on the Go integration with multiple banks *(currently ongoing)*

- Integration with multiple banks for caution money

ii. IFMS (with multiple states)

iii. PFMS

- E-Asset integration with PFMS

- E-Billing integration with PFMS

iv. Payment Gateways: e.g., SBI MOPS (Additional integrations with PayU, Bill Desk and other gateways proposed)

b. Lending integrations:

i. GeM Sahay: SAHAY is an online Platform that provides the loan against Orders and accepted invoices to the Sellers/ Service Providers. The GeM Integration with SAHAY platform aims to facilitate the loan to interested proprietors registered as Sellers/ Service Providers on GeM portal against the Orders that they receive from the Buyers on GeM. The order and Seller/

Service Provider details will be shared digitally through GeM SAHAY Integration from GeM portal to SAHAY. Along with the order information, the events occurring in the order lifecycle on GeM – CRAC generation, Bill generation and Payment Update notification would also be shared by GeM portal with SAHAY through the integration. The integration aims to fast track the loan disbursal to the interested Sellers/ Service Providers through the SAHAY Platform

ii. TReDS (bill discounting): TReDS is a platform which facilitate Seller to receive his invoice amount without getting affected by the delays in the payment processes at the Buyer end. GeM & TReDS has decided to offer this facility to GeM Buyers and Sellers/ Service Providers in the GeM platforms. TReDS has three different invoice discount platforms (RXIL, MI Exchange and Invoice Mart) where Sellers and Buyers are registered as participants. Each platform exposes the invoice to the member banks and based on the best rate offered in the platform, Buyer and Seller/ Service Provider, agree to selected bank's offer and Seller/ Service Provider gets his invoiced amount on discounted terms. On agreed due date, the Buyer pays the bank to settle the account. As per GeM terms, Buyer has to pay the Seller within 10 days of generation of CRAC. In case the Buyer is not able to meet their commitment, they can avail the facility of bill discounting via TReDS. As per the mandate, only invoices generated by MSE Sellers against PSU Buyers (Non-PFMS) will be exposed to TReDS platform. GeM shall not be storing any information related to bill discounting such as (a) Platform which facilitated bill discounting, (b) who is bearing the cost, (c) rate of interests etc. as these are handled by TReDS platform operators

c. Certification agencies: e.g., FSSAI, BIS, etc.

d. Logistics parties: e.g., India Post integration

e. Verification bodies: e.g., UIDAI, ITR services, GST portal, MCA-21, etc.

f. Inspection Authorities : e.g. QCI

g. Others: e.g., E-invoice (GSTN) integration with NSDL, SMS integration, E-mail integration

Following are the integrations proposed in the future and shall be considered as part of the scope of this RFP:

a. Integration with other Buyer's ERP systems

b. Integration with Single Window Interface for Facilitating Trade (SWIFT)

c. Integration with WhatsaApp

d. Integration with ERP systems of Self Help Groups, Weaver and artisans, TRIFED

e. Integrations with FCRA, FLLP

f. Inspection bodies

g. Provision for GeM platform to be made ready for onboarding ONDC as a Seller application

h. Lending integration with all Scheduled Commercial Banks as per RBI

i. IFMS integration with all states

j. E-invoice integration: Seller/ Service Provider should be able to generate e-invoice via GeM

k. Enhancement of integration with GST Portal to fetch e-Way bill data

l. ERP and SAP integrations with any other organization

m. Integrations with third-party systems such as airlines, hotels, taxi Service Providers, and other similar services *(as aligned with GeM)*

n. Integrations with Credit Rating Agencies (CRISIL, etc.) and other financial institutes/ NBFCs *(as aligned with GeM)*

MSP shall be responsible for the following, as per alignment with GeM during the design phase as mentioned in Volume 1 Section 5 of this RFP:

1. Implementation of all existing and currently ongoing integrations

2. Implementation of additional/ new integrations as listed above

3. Implementation of new functionalities/ interventions required within existing integrations

4. End-to-end testing of all integrations. Mechanisms to monitor issues with integrations shall be developed, including reconciliation reports, integration failure reports, error reports, etc. in order to monitor the health of the integrations

5. Ensuring all integrations comply with all relevant GoI/ ministry/ department guidelines such as RBI security guidelines

6. All costs, including one-time as well as per transaction/ recurring costs, pertaining to all integrations (per transaction/ recurring costs wherever applicable - e.g., UIDAI, GSTN, SMS, PAN, WhatsApp, etc.) shall be borne by the MSP

8.1.19 Certificate Authority and e-Sign Solution

GeM intends to implement a Certificate Authority and e-sign solution for the purpose of issuing e-sign and DSC for GeM users without any dependency on external parties. MSP shall be responsible for the design, supply, installation, commissioning, implementation, integration and support for Certificate Authority and e-Sign solution as per existing and future CCA guidelines.

"e-Sign" service is an online Electronic Signature Service in which the key pair generation, certification of the public key by the Certificate Authority and digital signature creation for electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services complying the IT Act.

The MSP shall provide all required functionalities, infrastructural requirements, with physical separation via air gap, as per guidelines defined by Controller of Certifying Authorities, and any other compliance required to make GeM certifying authority.

E-sign Service Providers, application Service Providers and e-KYC providers shall comply with all relevant guidelines, audit compliances, any other applicable compliance as per CCA, MeitY and IT ACT to enable authentication based on e-signing and DSC at various stages of procurement.

The design, development and implementation of the Certificate Authority and e-sign solution shall be done as per alignment with GeM during the design phase. The solution shall however include the following indicative features.

The Certificate Authority software solution shall have at least the following, but not limited to, major components and its mandatory features:

1. **Certificate Life Cycle Management Solution**

   A comprehensive Certificate Lifecycle Management Solution which should manage full life cycle of certificates of users, computers, servers and mobile devices in GeM. The certificate management solution must comply with all the hardware and software requirements mentioned in CCA guidelines and Certification Policy of India PKI Ver 1.6 Feb 2019 or any

latest guidelines if issued by CCA before signing of Master Services Agreement. The software shall have the following modules like:

a. **Registering Authority (RA) Module:** A web based application module meant for processing certificate requests. It allows the users to fill an online application form and download certificates to crypto tokens. It provides provision to RA and CA to validate the application form and then approve or reject the same. This module works in conjunction with CA module. For SSL Certificate issuance, high level verification as per existing CCA guidelines shall be carried out.

b. **Certifying Authority (CA) module:** This should be the Certificate Management Portal used by Issuing CA/Offline CA administrator for approval of certificates. CA will verify the details and approve/reject the application. If CA approves the application, certificates can be downloaded by the user. CA should have capability to revoke, suspend and activate requests.

c. **OCSP Responder module:** The module should be complaint with RFC 6960 or equivalent or latest meeting Indian standard for e signing compliance mandated by CCA , IT act, etc. with a web UI for generation and management of OCSP keys and certificates. The module shall also have the functionality to interface with logs real time

d. **Certificate Revoking List (CRL) Monitoring tool module**: A separate module/tool is to be available in the main module for checking the validity of CRL published by CAs. It should have provision to continuously monitor timely issuance of CRLs and its availability.

e. **Time stamping module:** The module should support generation of timestamps in accordance with RFC 3161 6960 or equivalent or latest meeting Indian standard for e-signing complinace mandated by CCA, IT act, etc.

2. The solution shall be capable of certificate issuance and management both in online and offline mode

3. The solution shall be web UI based application that ensures the security and scalability of electronic transactions by providing flexible, scalable systems for managing digital identities

4. The solution shall support X.509 v3 6960 or equivalent or latest meeting Indian standard for e-signing compliance mandated by CCA, IT act, etc. in compliance with RFC 5280 6960 or equivalent or latest meeting Indian standard for e-signing compliance mandated by CCA, IT act, etc.

5. The solution shall facilitate Certification Authority and User Certificate management that

includes option to issue, renew, revoke, suspend, etc.

6. The solution shall facilitate CA and user for certificate profile generation and management (Cloning of profiles, Ordering of Certificate extensions, and Subject DN details).

7. The solution shall facilitate creation, management, and publishing of Certificate Revocation Lists

8. The solution shall support various algorithms and key sizes such as DSA (1024), RSA (2048, 4096, 8192), ECDSA (256,384.521) or equivalent or latest meeting Indian standard for e signing compliance mandated by CCA, IT act, etc.

9. The solution shall support encryption such as enhanced key usage using symmetric key encryption algorithms like AES, 3DES (key stored in HSM) or equivalent or latest meeting Indian standard for e signing compliance mandated by CCA, IT act, etc. It shall also include encryption of databases

10. The solution shall support role-based access to the applications and should strictly follow the CCA guidelines

11. The solution shall support for mobile PKI using various platforms of mobile (window, Android, iOS etc.)

12. The solution shall have capability to create users, groups, and mapping of groups to CA/issuing CA for group wise management of CAs

13. The solution shall adhere to Protection Profile 1.5 version in Common Criteria Certification EAL4+ certification or equivalent or latest meeting Indian standard for e-signing compliance mandated by CCA , IT act, etc.

14. The solution shall support multiple HSMs (over PKCS#11 and JCE) certification or equivalent or latest meeting Indian standard for e signing compliance mandated by CCA, IT act etc. for storing CA private keys and all other system keys.

15. E-sign solution should have the following, but not limited to, features:

    a. eSign Software Solution shall have all the functionalities as mentioned in the latest CCA guidelines related to eSign

    b. The eSign Software solution shall have the following major modules:

        i.   User Enrolment module

      ii.   Authentication module

      iii.   Key Lifecycle management (Key Generation, Destruction)

      iv.   E-Sign Gateway

      v.   Administration module

c. The eSign shall comply with single factor authentication (biometric/OTP/fingerprint/face recognition) or Multi-factor authentication (OTP & biometric, OTP & Pin etc.)

d. The proposed solution shall provision UIDAI based KYC and organizational based KYC as per new CCA Government of India guidelines.

e. The eSign solution shall support all protocols to integrate with the GeM Applications as per the CCA Guidelines

f. The eSign Solution shall provide audit reports and audit logging as per the existing and enforced guidelines on eSign as per CCA, IT Act, etc.

16. The MSP shall take necessary actions for development and implementation of Certificate Authority and e-Sign solution and shall comply with the CCA guidelines for Certifying Authorities and eSign Service.

17. Audit:

a. MSP shall regularly conduct the audit of e-signing service by auditor empaneled by CERT-In /IS Auditor/ IS of e-KYC compliance requirements

b. Audit report should comply positively with all Audit requirements. No open comments / objections should be reported by the auditor.
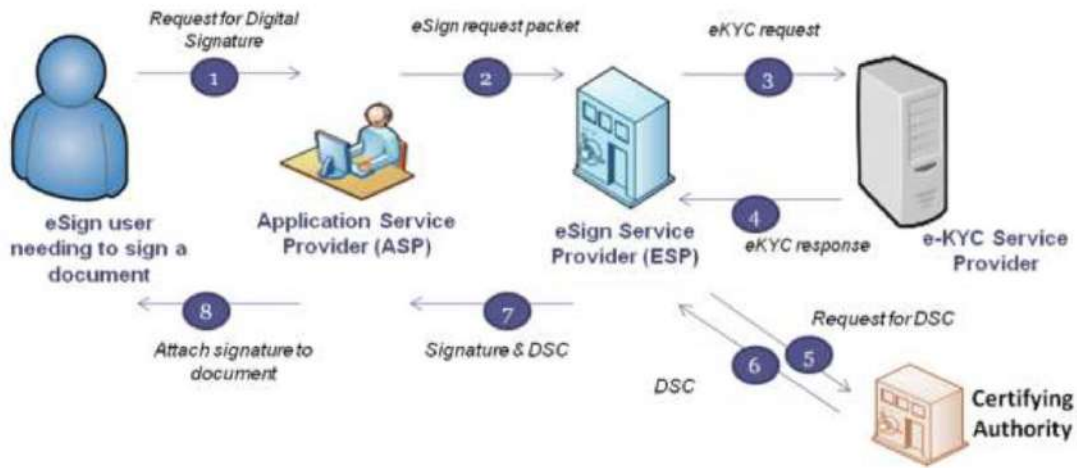
Figure 54: e-Sign Process

8.2 Annexure B - Technology Architecture

This section focuses on how the GeM system solution architecture should look like. The contents of the section are logically structured so as to make enhancements to this section as and when there is an opportunity, based on additional learning, to mature it to a higher level. The section provides the expected technical architecture of the GeM system. It was necessary to orient the section based on adopted international standards. The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture that provides a comprehensive approach for designing, planning, implementation, and governance of enterprise information architecture. While it will be expected that the elements of the solution architecture will be covered by the MSP, MSP should come up with their own suggestions on the solution architecture.

8.2.1 High-level design principles

The design for the solution architecture for GeM needs to follow the following broad architecture Principles:

1. Loosely Coupled Architecture

2. Scalable and Flexible

3. Repeatable and Reusable Components

4. Automate as much as possible: Real-time

5. Aligned with Business Strategies, Processes & Technologies

6. Cost-effective

8.2.2 Guiding Architectural Principles

IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks, and future state target architecture.

Desired architecture outcomes	Key technology requirements
Maximize the ease of integration with internal systems and with third party manufacturers and ecosystem players.	1. Definition, build, maintenance and consistent (re)use of **a library of secure public and private APIs** for integration of discrete systems, internal or external 2. **Standardized, flexible and configurable APIs** between packaged components.
Simple architecture through the establishment of integrated platforms	1. The end-to-end **architecture comprises a small number of pre-integrated solutions** designed to work together. 2. Components that are **designed for extensibility,** making it easier to adapt to future technology changes and innovate. 3. Robust and integrated **data management and insights capabilities** including **data quality framework** to support customer lifecycle data management as part of sales and service. 4. Implement **NoSQL databases**, where possible, for hosting of any large, structured data. 5. GeM middleware should implement a server side caching layer for faster data retrieval times as well as to reduce direct Database calls for any APIs or functions. 6. API Lifecycle Management shall be responsibility of the MSP
Enable fast, higher quality change delivery, in order to	1. The ability for **individual software changes to be independently developed, tested, and deployed**, e.g., modular code bases.

Desired architecture outcomes	Key technology requirements
meet changing customer needs more quickly.	2. Frameworks and software libraries that **maximize the potential for reuse**, e.g., of presentation screens, business logic, business rules, process flows, orchestration, and data. 3. **Mature DevOps processes and tools** to support rapid and effective development, delivery, and management of applications throughout the software development lifecycle. 4. **Configurable solutions** that allow common and recurring changes to be made by authorized business users without support from Technology for additional convenience and effort free implementation as well as prevention of hard coding of such values. 5. View Layer caching may be delivered via **Content Driven Network (CDN).**
Enhanced stability, scalability, reliability, and supportability to ensure systems are available when Buyers and Sellers need them.	1. Flexible and adaptable **integrated cloud-enabled hosting models** (either private or public). 2. Dynamic adaption to workload changes through **elastic provisioning and de-provisioning of resources.** 3. Levels of **redundancy consistent with the business value-at-risk** from unscheduled outages. 4. **Integrated support tooling** to provide monitoring and traceability of end-to-end transactions, performance metrics, security events and overall solution health. 5. **Serverless deployment** (container based) may be implemented to ensure higher utilization and elastic scaling up and down of resources. 6. All **live services should be adequately monitored** to respond to downtime and errors in the system. System should be able to capture all error codes in APIs and alert the system team in real time.
Rigorously protect the security of the data entrusted by Buyers and Sellers	1. System access based on well-defined and flexible **role-based user access model.** 2. Maintenance of a **robust information security environment,** to prevent the unauthorized disclosure, duplication, modification or deletion of customer data.

Table 85: Architectural principles

The GeM system would be built on the following core principles:

#	Principle	Description
1	Open IT/ Ecosystems	1. Well defined APIs are designed with open standards. 2. Easily integrate new systems, FinTechs, disruptive tech, etc. 3. Standards-based and open. 3. Enable new ecosystems/partners to extend the breadth and depth of offerings
2	Minimizes Architecture Complexity	1. Only one component supports a business capability. 2. Use applications/tools for core purposes, not for what it can do. 3. The low number of platform vendors delivering related capabilities. 4. Pre-integrated components are designed to work together. 5. New vendors/services are only introduced if the capability is not available from the existing platform or is differentiating.
3	Industrialized / Rapid Delivery	1. Supports modern engineering practices (DevOps, Agile, Containerization). 2. Frequent, incremental, and instantaneous updates are in line with the platform roadmap. 3. Consume non-differentiating "Utility" services via API.
4	Configurable & Extensible	1. Business self-service for BAU changes (configuration changes). 2. Extensions do not compromise the upgrade path. 3. No customization. Solutions are used out-of-the-box.
5	Scalable (Cloud where feasible)	1. Can be supported in private and public clouds. 2. Available in an 'As a Service' model – available and scalable. 3. Scales up and down easily for consumption peaks and troughs.
6	Information-Centric	1. Uses data and insights to drive behaviour (UI,). 2. Easily shares information and insights across the architecture. 3. Systems must publish their data with technical and business metadata. 4. Reduce latency of data ingestion and consumption and maximize reuse potential (the right data at the right time). 5. Configuration-driven and self-service data integration services. 6. Data consumption services to enable reuse of integrated data, reduce uncontrolled growth of 'stovepipe solutions' and enable flexibility for self-service consumption.

#	Principle	Description
7	Stakeholder Centric	1. Solutions must span channels, no channel/product silos. 2. Consistent stakeholder experience across channels. 3. Employee interaction with solution/customer well addressed.
8	Manageable & Supportable	1. Activity can be tracked end-to-end. 2. The platform supports continuous availability, can be updated without downtime. 3. Supports phased implementation of new features (A/B).
9	Compliant, Secure and Reliable	1. Data collected, stored or processed meets the data protection policies and is managed and backed up in accordance with data management policies. 2. Designed with the principle of least privilege – provide role-based access to information and resources for consumers or services where a legitimate purpose is identified. 3. Ability to support discrete asset/function security model, e.g., Micro-Service security.
10	Cloud	1. Minimize cloud lock-in with placement agnostic technologies such as containers or common cloud services. 2. Support application delivery controller technologies; global load-balancer, traffic proxy, etc. for cloud workload control. 3. Ability to use service discovery mechanisms for transparent, loosely coupled service integration such as Consul, LinkerD or Istio.

Table 86: Core principles

8.2.3   Solution Architecture

The GeM platform should be highly flexible microservice architecture in order to satisfy business requirements with short time to market and minimum disruption. The target state architecture should cover three aspects: architecture, software design and DevOps

1. Define the architecture with an API layer to decouple services

2. Adjust the software design of the existing monolith to be modularized and to allow parallel development

3. Introduce DevOps and automate everything into a highly flexible cloud container solution to get the services into the market as quickly as possible

Each aspect should cover specific tasks in order to enable microservices across GeM functional modules.

Architecture:

1. Identify the business domains of the application landscape

2. Define business driven API landscape along the identified business domains. Can be done incrementally while refactoring the monolith

3. Encapsulate the monolith with thin microservice layer to provide the defined business driven APIs

4. Define robust guidelines for the integration of the microservices (i.e., RESTful)

5. Introduce an API management platform to provide a common set of functionalities

6. Define the allowed database and storage patterns

7. Define data archival design as per the data archival policy

Software design:

1. Detail each business domain into different contexts in the application

2. Separate the contexts into logical blocks

3. Build the logical blocks as modules

4. Carve out modules from the application as microservices

5. Do this incrementally

6. Separate the frontend from the backend layer if those are currently combined in a full stack application.

DevOps and automation:

1. Introduce DevOps methodologies and mindset

2. Automate integration, testing and deployment with CI-CD pipeline

3. Automate infrastructure provisioning with cloud technologies

4. Use containerization to maintain separation between the microservices (Docker, Kubernetes)

5. Set up central logging and monitoring to get rapid feedback about usage, errors and cascading failures (can be provided by API gateway)
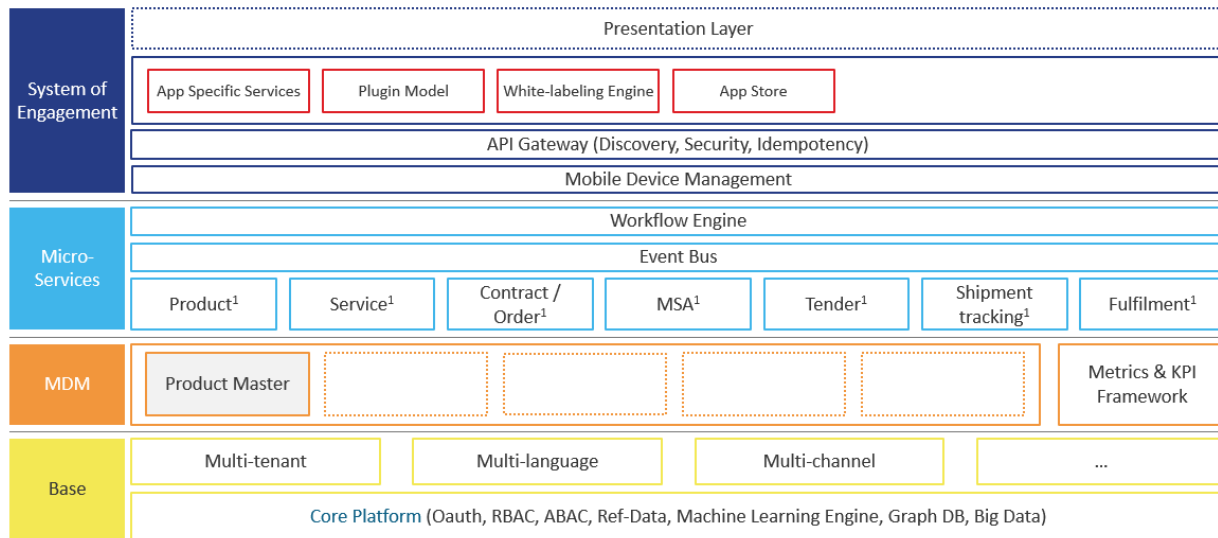
Figure 55: Proposed multi-layered target state platform architecture for GeM (Part 1)
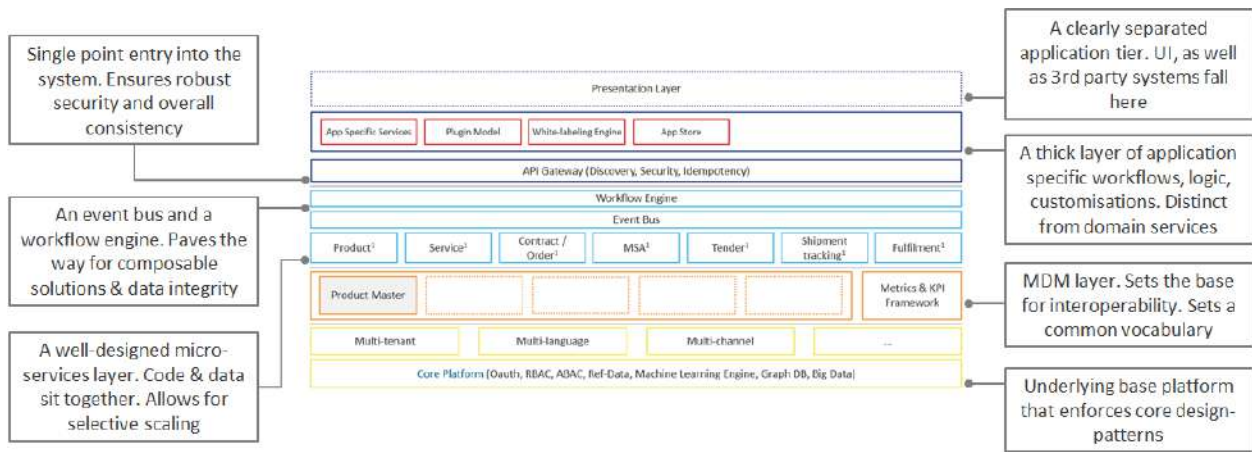
1. Illustrative services – need to be finalized once target domain model is ready

Figure 56: Proposed multi-layered target state platform architecture for GeM (Part 2)

GeM platform should go for complete transformation by defining a layered architecture with well-defined components.

1. The target architecture is expected to have well defined layers of responsibility. Each layer is expected to implement a specific purpose and should not overstep its responsibilities such that it encroaches the responsibilities of the other layer.

2. The layers are expected to communicate with each other using well defined protocols and data structures. No hard dependencies between the layers should be there.

3. In the following sections, we have provided an overview of the responsibilities / architectural considerations for the various components contained in the layers in question.

8.2.4 Users

The key users for the proposed system would be from Government Buyer departments, the Sellers or Service Providers and internal users of GeM. User creation can be a self-service facility with an approval workflow approved by a competent authority. The application will be accessible to the following users:

1. GeM internal users

    a. GeM Buyer Management Team

    b. GeM Seller/ Service Provider Management Team GeM Product Owner

    c. GeM Service Owner

    d. Contact Centre

2. Government Buyers

    a. HoD/ Primary Buyer

    b. Procurement Officer

    c. Consignee

    d. DDO/ PAO

    e. Technical Evaluator

    f. Indentor

    g. Other user roles created in the future (Competent Authority, Verifying Authority, junior procurement personnel, legal and finance officers, etc.)

3. Suppliers / Sellers / Service Providers / contractors

4. Partners: The key partners for the system would be various organizations such PFMS, IFMS, Banks (including bank wallets), Payment Gateways, NIC, Ministry of Corporate Affairs, Tax agencies like Income Tax Department, GSTN, CBIC and State Tax Departments, UIDAI for Aadhaar services, MCA-21 for Company verification purposes, etc. The seamless integration

with these partner systems would enable automated validation and verification of suppliers or Buyers who want to be a part of the GeM system, payments, and smooth, reliable and real time functioning of the other business processes on GeM.

5. Third Party agencies: Third party agencies envisioned to be integrated with GeM are inspection agencies, credit rating agencies, logistics players, Chartered Accountants, and others as per requirement. They will be responsible for different work streams, which may be outsourced to them, e.g., credit rating agencies for providing financial health of supplier, inspection agencies for conducting inspection of products & Services and Chartered Accountants for authentication of supplier registration & tendering related documents.

The information dissemination on the GeM system shall be done through SMS and email. The GeM application shall be available to its users through mobile client and web browsing channels. Key business capabilities that need to be created or modified are mentioned in Volume I Section 8.1 of this RFP.

8.2.5 Domain Layer

The Domain layer should comprise of 6 essential sub-components:
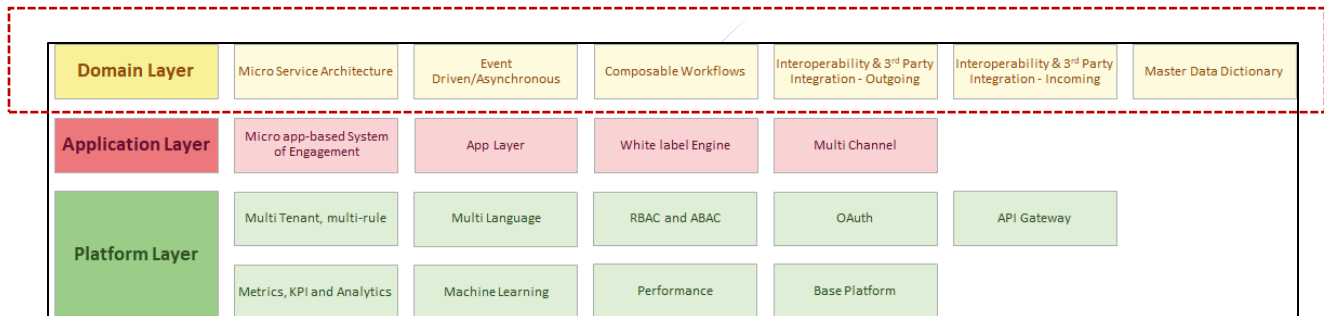
Figure 58: Domain layer of target state platform architecture for GeM

1. Microservice architecture:

   a. The architecture should be developed in order to have essential architectural elements - Code & data isolation with centralized configuration" , " Service discovery, registry and centralized monitoring" , " Horizontal scalability, automated deployment"

   b. The target architecture needs to be domain driven, and merely based on the specific needs to each screen of the UI.

c. Separate code and data-isolation (database schema) for each domain services adhering guidelines of domain driven design

d. Each microservice should have well defined domain boundaries. Services need to be highly cohesive and should not step over the functional boundaries of another service.

e. There should not be any hard dependencies or hard relationships between entities belonging to separate micro services. Only soft dependencies will be maintained between entities of different micro service

f. Each domain service should perform its transaction and publish an event. The consumer should listen to the event and perform transaction. If the transaction fails for some reason, a failure event should be thrown to rollback transaction in other service.

g. During varying traffic needs for read and write operation, target architecture should support Command Query Responsibility Segregation (CQRS) principle.

h. For high availability, each microservice should be able to scale horizontally and shared global data should be handled through distributed cache

i. Each microservice should have separate code base in version control system.

j. Each microservice should have separate schema with access to its own schema.

k. All microservice should be configured under CI-CD pipeline for build steps and when deployed, it should fetch configuration from a central config server.

l. All microservices should register their availability status, base-URL to a central service registry allowing other microservice to communicate.

m. The architecture should be defined for an event driven system

n. The architecture should be horizontally scalable – using the principles of CQRS, events and composable workflows.

o. In order to share master data and configuration, distributed cache should be implemented. Container orchestration tool to support cluster deployment with failover mechanism to switch from node to node in case of failures.

p. Microservice deployment should happen through CI-CD(continuous integration,

continuous deployment)

q. Architecture should have monitoring and fault tolerance using log tracing mechanism with unique trace ID's to keep track of requests being routed to multiple services.

r. Target architecture should implement capabilities to aggregate logs from different microservice to a central log viewer for easy access and analyze. This implementation should allow to search, filter logs based on service id, log levels, origin, timestamp etc.

s. The microservice architecture implementation should have well defined strategies for fault tolerance. This fault tolerance architecture should ensure fault tolerance by ensuring, a strict timeout policy per request from waiting forever, a circuit breaker policy preventing repeated failure by setting some condition to activate circuit breaker.

t. The architecture would work with events generated from various state/process changes, in turn would inform the related services.

u. Each service should subscribe to events with event data in well define data structures.

v. Interaction between the services would happen via events, composable workflows. The architecture would not facilitate any point-to-point interaction between the services.

w. In order to save all the changes to the data state, event store has to be defined, in order to capture the state change in the form of event streams. Some of the most popular event stream engines like Kafka, AVRO can be leveraged.

x. In order to orchestrate complex business processes, composable workflows using workflow/BPMN engine to be build. This would avoid hardcoding of workflows in the microservices. Some of the off the shelf workflow components like Camunda could be directly used with GeM specific tailoring

y. Workflows would be exposed using REST API based interface, will be independently deployable and testable.

z. Standardize definition of data dictionary to form a uniform repository of master data elements to be referenced with all the GeM service & 3rd party systems.

aa. The master data dictionary would establish a common vocabulary for internal and external communication. The data elements would include product codes, data codes for product specs, geo-codes, etc.

bb. MDM system should implement a hierarchy between related data which employs parent and child relationship. An example would be state and district.

cc. Master should have standardized format and should be readily available to all components.

dd. Master data should be present in distributed cache for faster retrieval

ee. Master data management should support multi-lingual for displaying labels in vernacular language

8.2.6 Integration Layer

8.2.6.1   Integration with External System

Many external systems would need to be integrated with GeM to achieve digital, paperless kind of ecosystem. GeM platform integration process should work for inbound and outbound data exchange mechanism with external systems.

1. For the outbound integration process, usage of process automation with well-defined contracts (via channel adaptor) and usage of proxy pattern by defining a contract layer. The contract layer should be kept different from the domain service layer to ensure loose coupling between invocation from domain service to 3rd party system and its implementation.

2. For inbound integration process, a well-defined interoperability framework needs to be built in the architecture framework:

   a. Definition of data interchange standards,

   b. Master Data Codes, and

   c. Requested signatures that can used to integrate with the GeM platform.

The platform should ensure definition of standard interfaces, data-formats, and protocols. In order to exchange data and services securely – modular webservices to be exposed by GeM platform & API gateway to as single point of entry and exchange for any 3rd party data exchange.

Integration Technologies that are recommended to be used are:

1. JSON/XML based data exchange on RESTful Microservices API/Thrift API

2. Standardized API structure/ framework as exposed by GeM to be consumed by external systems.

3. Proprietary contract layer (channel adapters) for e.g., JMS, web-services, etc.

Connection with external applications should be provisioned via a common messaging system using messages of a pre-defined format. The messaging style should maximize decoupling between systems not only from the interface perspective but also from a time-based perspective. Some of the common patterns to be followed – Pub/Sub, Event message, channel adaptor.

Replication technologies for replication of data between different data stores:

1. Interfacing mode for GeM platform will be leveraged as the real-time in most of the cases, while file transfer & point to point in some cases. The messaging could be synchronous/asynchronous with external or third-party systems. The following integration target points could be considered for interface design :

   a. Payment gateway of the authorized banks to enable authorized users make financial transactions for the GeM services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.

   b. SMS application, acting as the SMS Gateway, will make use of Java Communication APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time-driven. The API will be exposed to initiate the broadcasting or alert notification.

   c. IVR/Customer Support solution to exchange business demographic, registration, and payment data as well as transactional data related to the e- Market place related activities.

2. Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message-based interfacing:

   a. Central LDAP may be used to synchronize member and user registration data

   b. Payment gateway to exchange payment data for tracking of beneficiary's payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)

c. Departmental applications may be used to exchange data for procurement and maintenance of any assets or infrastructure items for each department.

3. RESTful API service-based interfacing technique will be leveraged for the following integration areas -

   a. Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.

   b. Access and use of various internal functions related to operations and administration of GeM for departmental and GeM employees will be done through a RESTful, stateless API layer

4. Data integration in batch mode will be through ETL using dimensional modelling and data pipelines. The following integration points could be considered for ETL data integration -

   a. Initial data migration to cleanse, validate and load the data extracted from source systems into target tables

   b. Only Incremental data load from all the individual transactional systems to central enterprise data warehouse solution for aggregation, mining, dashboard reporting and analytics on periodic basis for e.g., daily/weekly/monthly refresh cycle. The incremental load should be based on the data updated in the respective systems

8.2.6.2 API Gateway Services

It is expected that the communication of the GeM services – domain, application and workflow engines with external interface will happen through an API layer. An API gateway to be used as single point of entry to manage the API communication with the external interfaces. Following are some of the expected features for API management using API gateway -

1. All access to the GeM platform backend system will be via microservices. Access to microservice will be via an API gateway.

2. API gateway can be implemented using available tools provided by the cloud partners – AWS, NGINX, ZUUL, Spring cloud gateway are few popular ones.

3. API gateway should implement cross cutting concern like logging of request, idempotency, request throttling, security for request authentication, monitoring/metrics across microservices.

4. The API gateway implementation should be based on reactive programming model with circuit breaker integration, load balancing, service discovery.

5. API gateway implementation should have an ability to match routes on any specific routes, pre and post filters which can be either global or specific to any routes.

6. All the APIs would be stateless in nature, thus easy to load balance, even if hit through portal is very high and this requires high end processing.

7. All the APIs, both internal and external, should be on HTTPS or secure protocol

8. The API gateway should be allowed to manage all enterprise initiatives from a single solution.

9. The API gateway should support existing APIs and developer preferences and provide the features in line developer preferences.

10. The API gateway should provide clustering and ensure reliability, scalability, and single point of administration :

11. The API gateway should provide for enterprise grade encryption:

12. The API gateway should provide secure access to all APIs and provide ALL the forms of authentication, access control and certificate/credential support:

13. The API platform should provide comprehensive threat protection for all API traffic.

8.2.6.3   SMS Gateway adaptor

SMS services are envisaged to be made available as part of the solution design. The contract layer hosting the SMS gateway channel adaptor to be used for calling the SMS service.

SMS services can be used for OTP authentication and as well as informing the users about their registration status, payment alert, return update, etc. The Service Provider may integrate the solution with MSDG, and use the services available through it, or deploy SMS Gateway services developed by it for GeM or integrate with other SMS gateways provided by Service Providers, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution.

For outbound message SMS gateway can be developed. Specifications related to SMS gateway are as below:

1. The gateway must be as per prevailing TRAI/DoT norms

2. Should contain required details /information and targeted to the applicant or designated officers of tax departments and other stakeholders

3. Support automated alerts that allows to set up triggers that will automatically send out reminders

4. Provide provision for International SMS

5. Resend the SMS in case of failure of the message

8.2.6.4   Email Services adaptor

The contract layer uses email channel adaptor to call the email services. Email services are envisaged to be made available as part of the solution design to send alerts / intimations / automated email messages to the registered email ids, based on preferences set up / opted by individual users.

An authenticated SMTP mail service (also known as a SMTP relay or smart host) shall be provisioned to be integrated with the GeM platform for sending mail from the platform, delivered to intended inboxes and support antispam features.

8.2.6.5   Integration with SSDG, NSDG, National Portal and MSDG

MSP shall support integration of GeM solution with SSDG, NSDG, National Portal and MSDG respectively, as per NeGP guideline and DeitY, and actual requirements of GeM platform. GeM platform whitelisted APIs are required to be adjusted to accommodate additional fields only (base API construct remains intact) to cover specific business logics.

It is mandatory that the requirements of 'Integration' and 'Scalability' must be considered while developing /customizing the application so that any change is easily addressed as and when these systems are implemented at the state and national level.

8.2.7 Security Architecture

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of GeM security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the involved stakeholders. The security controls are defined for 6 layers, namely, Business, Data, Application, Perimeter, Network and End-point.

For designing GeM's Security Architecture, following principles need to be adhered to:

1. Data Integrity: GeM data must be correct, consistent and un-tampered

2. Data Privacy and Confidentiality: Information needs to be shared on a Need-To-Know basis and shall be collected/accessed/ modified only by authorized personnel

3. Non-reputability: GeM should ensure non-reputability of information in the system

4. Secure by Design: Security has to be built into all stages and all aspects of architecture development, based on Zero-trust principle

5. MSP shall be responsible for meeting project's comprehensive security requirements and 24*7*365 monitoring, analysis and management to ensure adequate security posture & security compliances as part of its security operations activities (ideally through a SOC). However, GeM reserves the right to further appoint an external agency for monitoring the compliance to security requirements by the MSP. The external agency shall have access to security tools deployed by MSP (at no cost to GeM) as part of the RFP

8.2.7.1 Business Layer

Based on the business requirements GeM should develop policies and procedures to be followed to have secured solutions. Risk assessment, stakeholder identification, asset identification, the requirement of every service and application, various standards and statutes followed by the GeM are required while designing security policies. At the business layer management should do risk assessment followed by the impact analysis of these risks to identify appropriate controls and define them in the security policy document.

8.2.7.1.1 Defining Policy

1. Responsibilities of GeM

   a. Develop the security policy to address threats and vulnerabilities. MSP would need to advise and comply with the policy

   b. Identify the resources to implement, monitor and update the security controls as per the defined policy

   c. Define the schedule of regular testing and monitoring to maintain to ensure all-time security

   d. Define the access controls at various levels such as data centre, application, data, network, periphery layers

2. Responsibilities of MSP

a. Define authentication mechanisms at various levels as per the business requirements

b. Define compliances related to endpoint usage

c. Define cryptographic standards to be followed along with the recommended key management policy

d. The security policy document should be published and made available for ready reference for all the concerned

8.2.7.1.2 Functionality at Business Layer

1. Security architecture and design: A proper security architecture considering all the components as per the reference model should be in place and configurable design to meet the objectives of the overall security of the enterprise.

2. IT security governance: This comprises of formulation of guidance, structures, and processes for implementation of IT policy, risk, compliance, and audit functions.

3. Threat Modeling: What are the threats and what can be their sources should be identified? In order to do threat modelling identification of assets and related vulnerabilities is crucial.

4. Risk assessment and management

   a. Assets should be first identified and then the Inventory of assets should be maintained. Acceptable use of assets should be documented and ensured that it is implemented in every project.

   b. Information should be classified as per its sensitivity and risk associated with the information such as data leak, privacy etc.

5. Vulnerability assessment and penetration testing: The objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation. A policy should be defined by the departments to foresee the possible vulnerabilities and simulation of exploiting those vulnerabilities. VAPT is usually being discussed for exploiting the security of the application servers, network and the running application. However, it may also be seen for other layers as well such as the possibility of spoofing in the installed biometric sensors which are being installed for the purpose of preventing unauthorized access to the physical systems.

6. Security technology evaluation: The objective of security technology evaluation is to

determine the degree of compliance with a stated security reference model, various controls, standards and specifications. For example, Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security; Information Technology Security Evaluation Criteria by European Union for evaluating enterprise security are being used extensively.

7. Continuous monitoring and analysis: It is not only defining the policies, standards or referring of the various international security standards but also defining the metrics which should be monitored and analyzed on a regular basis to achieve the required quality for security.

8. Security training to build awareness: There is a need to develop a proper plan, policy to create awareness, capacity building for achieving the desired security for an enterprise.

9. Incident detection and handling: The purpose of incident detection and handling is to determine the possible attacks/threats to the overall system. Vulnerability at any level of the reference model can lead to a threat to the overall enterprise. There should be a mechanism to identify that vulnerability and the procedures to handle them. For example, vulnerabilities related to network security, physical access to the systems, data access management etc.

10. Continuous certification and accreditation of policies

    a. GeM should conduct the audit at regular intervals to verify the conformities. Agencies like STQC will be appointed for auditing and MSP should fully support to ensure that the audit is completed smoothly and on-time.

    b. The objective of the audit should be made very clear to the auditors.

    c. The report of the audit must be reviewed by the management for action and up-gradation required.

    d. Non-conformities identified during the audit should be addressed and used for corrective action as well as improvement in the policy.

11. Escalation management of security incidences

    a. All information security roles and responsibilities should be identified and allocated to the appropriate people.

    b. Appropriate contacts with the relevant authorities should be maintained.

    c. Maintaining a security dashboard

8.2.7.1.3 Business Layer Controls

Some basic controls related to the business layer are mentioned in this section. This is to be noted that the list of controls defined in this document is not a complete list but a guideline only. More controls should be defined as necessary. The below table provides the list of essential controls at the business layer of the security model.

Business layer controls	Description
Access Control Policy	1. A policy should be established, documented and reviewed as per the business information security policy to provide access to information or assets available at the state/ organization/ department level. 2. The policy should define who can access what resources and what authentication mechanism should be used to provide the access. 3. Different multi-factor authentication mechanisms should be defined for accessing different information and information facilitating resources based on sensitivity. 4. The principle of **'Least Privilege'** shall be followed, so as to give only the minimal permissions and authorizations to any user to enable him/ her to perform the specified functions.
Strong password	1. The policy should define what is an acceptable password. A strong password is recommended with a minimum of 8 characters, with at least one capital character, at least one numeric ad at least one non-alphanumeric character.
Professional/ company email id	2. It should be mandated that for all the official work only the company / department email ID should be used. No government information is to be shared on personal email IDs.
Incident reporting and handling	1. A mechanism should be defined and made available to detect any security-related incident. 2. A procedure should be well defined and documented giving steps to be taken for handling any incident.

SIEM	1. SIEM has two components, SIM (Security Information Management) and SEM (Security Event Management). It should provide real-time analysis of the security alerts generated by network hardware and applications. 2. A software information and event management system should be defined and documented for handling security-related incidents.
Learning from the security incidents	1. Knowledge gained through analysis of the earlier incidents should reflect in the security policy document.
Continuous Monitoring	1. An institutional setup consisting of information security experts should be established for continuous monitoring that can help in detecting any security-related incident. 2. The monitoring also includes the analysis of all actions and detection of the integrity getting compromised anywhere in the enterprise.
Policy for cryptographic control usage and key management	1. The security policy should include the use of cryptographic controls to ensure the confidentiality and authenticity of the user as well as systems. 2. The security policy should document the secured use and storage of cryptographic keys. 3. The cryptographic keys should be changed at regular intervals. The security policy should define the interval at which the keys are changed. The policy also should document the key generation mechanism to be used

Installation of software	1. A secure procedure should be defined for installing software.
	2. Rules governing the installation of software should be defined and implemented.
	3. Vulnerability Assessment and Penetration Testing (VAPT) should be mandated before installing any software in the production environment. Many CERT-IN empaneled agencies do VAPT testing of applications.
	4. Separate development, testing, staging and production environments should be recommended.

Table 87: Business layer controls

SIEM

Even after the risk analysis, identification of threats and providing controls, security breaches may happen. These are referred to as security incidences. There should be a well-defined mechanism to detect such incidences and reporting of these. Such incidences are analyzed by professional bodies such as CERT-IN. The professional body after analysis of the incidence may publish advisory. The security policy should be modified as per the recommendations given in the advisory. Updated security documents should result in appropriate controls at various layers to prevent the re-occurrence of the incident.

8.2.7.2 Perimeter Layer

Access to any software is restricted first through the hardware where it is deployed. The environment in which the data and the application reside should be protected first. Physical security is vital in order to protect the information and resources from unwanted access and intrusion.

8.2.7.2.1 Functionality at Perimeter Layer

The main functionalities at the Perimeter layer are to identify the appropriate security for every asset, application/service and data. Based on the policies defined at the business layer regarding the access to various assets, the appropriate configurations at various levels should be done at this layer.

1. Secure DMZ – Design the network considering the sensitivity zones mentioned in 'Designing of Network'.

2. IDS/IDP – Intrusion detection and prevention at the physical layer

3. Firewalls – to protect the infrastructure from unwanted or blacklisted intruders.

4. Message Security (anti-virus, anti-malware) – Appropriate anti-virus and anti-malware should be identified and deployed. Policy regarding the same should be made to inform all the concerned.

5. Data Loss Prevention

6. Buffer Overflow Exploit Protection

8.2.7.2.2 Controls at Perimeter Layer

The table below gives some of the important controls that should be considered while designing the security at the data centre.

Objective: Secure areas- To ensure that the information and the assets are not accessed, altered by unauthorized users through securing access to the physical infrastructure and the environment.		
1.	Physical Entry Controls	Secure areas should be protected using appropriate controls. Not everyone should have access to the data centre.
		An SOP should be defined for access to the data centre and different areas within the same.
		A proper access control mechanism should be defined and implemented.
		Multi-factor authentication is mandatory.
2.	Security of network services	Security mechanisms, service levels, and management requirements of all the network services should be identified and included in the service level agreements.
3.	Avoid single point of failure	In-network paths between users and critical IT system resources, all the links, devices (networking and security) as well as servers should be deployed in redundant configurations (also known as High Availability – HA).

Table 88: Perimeter layer controls

A data centre may have physical servers or a cloud setup. In the case of physical servers, the controls related to access will be more crucial. Data privacy and security are more of a concern in the cloud setup. Cloud security requirements have already been defined in Volume 1 Section 8.3 of this RFP.

8.2.7.2.3 Cyber Intrusions and Security Controls

The rate of cyber-crimes has increased drastically as the usage of online applications through various channels is increased. Different techniques are applied to prevent cyber-crimes which include the access control mechanism, providing only authorized access, putting restrictions on the use of assets, applying different techniques to secure the data in storing or in transition, intrusion prevention systems etc. Still there remains the possibility of intrusion and it should be detected and then managed. For detecting such intrusions intrusion detection mechanisms are used at the information level. Once the incident occurs, it should be managed and the changes in the security controls should be done accordingly. Controls related to incident management are given below. Cyber security controls are required at the perimeter, network as well as end-point layer.

Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
1.	Responsibilities and Procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
2.	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
3.	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
4.	Assessment of and decision on information security events	Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.
5.	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
6.	Learning from information security Incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

| 7. | Collection of evidence | The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. |

Table 89: Management of information security incidents and improvements

8.2.7.2.4 Audit

An internal audit should be conducted by MSP at regular intervals to monitor the security of the system and applications/ services. MSP should have well-defined requirements and should conform to a certain standard, and to ensure the conformance to various defined security policies and as a preventive measure of prevalent security threats, a security audit should be performed.

1. The goal should be defined for the audit. For every audit criteria and scope should be well defined.
2. The organization should define a plan, frequency, method, and reporting structure for the audit. While designing the audit program importance of the process should be taken into consideration, results or reports of the previous audits should be considered.
3. While designing an audit report the requirement of the management, its relevance to the management should be taken into consideration.
4. Various audit reports should be preserved for reference.
5. Selection of the auditors should be done impartially, and the objective should be the prime concern of the audit.

Audit Considerations		
Objective: To minimize the impact of audit activities on the production environment.		
1.	Audit Controls	Audit activities involving verification of systems in the production environment should be carefully planned to have minimal disturbance to the business or service.

Table 90: Control related to audit

While performing the security audit of services or infrastructure, the testing is performed on the production environment. Hence, it should be designed carefully that will not affect the services.

8.2.7.2.5 Recovery Strategy

Disaster recovery is an important aspect of information security. In the case of any natural or man-made threat, the earlier data should be made available.

Availability		
Objective: To ensure the availability		
1.	Availability of Information facilitating infrastructure	Information facilitating infrastructure redundancy sufficient to make the availability requirement of the application should be ensured.

<div align="center">

Table 91: Recovery controls

</div>

Business requirements for the availability of the service/ application/ information system should be identified. In order to ensure 24 X 7 availability, a redundant infrastructure should be identified. This infrastructure should also be tested for failover mechanism.

8.2.7.3   Network Layer

The perimeter layer covered the storage aspect of the application, service or data. However, the data in transit needs to be secured through the network layer. Many functionalities at the perimeter and the network layer are common.

8.2.7.3.1 Designing of Network

Network Security is critical for IT systems and their proper operations as most applications work in the networking environment and closely depend on network performance, reliability, and security. Improper network design can be very expensive i.e., loss of business, data loss, security breach, costs of network restoration, etc. Essential to network design is the security architecture that describes the network segmentation (i.e., security zones) and security layers (i.e., access control, intrusion prevention, content inspection, etc.).

8.2.7.3.2 Logical Network Segmentation

The network should be designed as "Zero Trust network" based on the trust level requirements of the application or the department or the service. While designing a network, the first one should identify different trust level applications or systems.

1. Untrusted zone (Internet / Outside Access) - It is the zone through which the organization/ department/ state connects to the outer world of the internet through Internet Service Provider (ISP).

2. Low Trust (External) - The systems deployed in this zone should be tightly controlled and hardened to reduce the attack surface. External DMZ has systems that are exposed to the internet for public access such as web servers, email gateways, FTP servers, web proxy

servers, remote access servers.

3. Medium Trust (Enterprise/ Extranet) - The Enterprise zone is where end-user systems reside, including end-user workstations, printers, and VoIP Phones. Endpoint protection is critical to limit the exposure of end-user systems to malware.

The Extranet zone connects with highly trusted third party business partners. Nonetheless, it is recommended that traffic between Enterprise and Extranet zones is monitored and filtered at the zone's perimeter to allow only approved traffic to enter and leave the zone. Systems in the Extranet zone will typically not abide by the organization's security policies. Therefore, it is important to perform a 3rd party risk assessment before establishing connectivity to understand their security posture and possibly strengthen perimeter defenses.

8.2.7.3.3 Functionality at Network Layer

The network layer ensures channel security and has to implement the controls as per the security policy at the network layer.

1. Network Access Control (NAC) – Provide endpoint security technology, the user or system authentication and security policy enforcement.

2. IDS/ IPS – IDS monitors a network or systems and identify malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identify suspicious activity, log information, attempt to block the activity, and then finally report it.

3. Firewall - Prevent unauthorized internet users from accessing private networks connected to the Internet. Basically, they do stateful packet inspections.

4. VoIP Protection - VoIP share the same infrastructure as the traditional data network, therefore inherits all security problems from the data network. VoIP does not have a dominant standard so far. Hence suitable measures should be taken for its protection.

5. Content Filtering - Screen and exclude from access or availability, Web pages or e-mail that are deemed objectionable.

6. Message Security - Message security uses the WS-Security specification to secure messages. i.e., ensure confidentiality, integrity, and authentication at the SOAP message level (instead of the transport level).

7. Wireless security – Prevent unauthorized access to the network using wireless networks. Common protocols used are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

8. Remote Access Security – Implement remote network access safely and easily to a wide range of users and devices.

9. Data Loss Prevention – DLP make sure that end-users do not send sensitive or critical information outside the corporate network. It also describes software/hardware products that help a network administrator control what data end users can transfer

8.2.7.4 Endpoint Layer

Services or applications are accessed using laptops, desktops, mobile devices etc. In addition to these currently many biometric devices are used to capture fingerprints, IRIS of the users to authenticate them using Aadhaar. For digital certificates, crypto tokens are used. All these devices are referred to as endpoint devices as these are used by the users. This section emphasizes endpoint device security.

8.2.7.4.1 Functionality at End Point Layer

Endpoint devices should be protected from various threats. Below care should be taken to do so.

1. Desktop level firewall – Protect the integrity of the system from malicious software code, filter inbound and outbound traffic, and alert the user to attempted intrusions. Should be enabled on every desktop in the network.

2. IDS/IPS - HIDS monitors systems and identify malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identify suspicious activity, log information, attempt to block the activity, and then finally report it.

3. Anti-virus and anti-malware – Every system should have the latest and updated version of suitable anti-virus and anti-malware installed. It detects and destroys computer viruses, malware and other malicious software code.

4. Compliance with Govt. Desktop Core Configuration(GDCC) – Servers and Desktops in the network should comply with the list of security settings recommended by GDCC.

5. Patch management – Security patches of various software should be regularly updated.

6. Data Loss Prevention - DLP make sure that end-users do not send sensitive or critical information outside the business network. It also describes software/hardware products that help a network administrator control what data end users can transfer.

8.2.7.4.2 Controls at End Point Layer

Mobile Device		
Objective: To ensure the secure use of the mobile device.		
1.	Mobile device policy	There should be a policy defining the security measures for using mobile devices. The devices should be protected with anti-virus and anti-malware.
Biometric Device		
Objective: To ensure data integrity and privacy in the use of the biometric device.		
2.	Biometric device policy	The Biometric Database of Aadhaar is very frequently used to authenticate users for various activities. The devices that are used to capture the biometric information should be secured against the loss of data or illegal access to the biometric data. Aadhaar act should be followed while using these devices for Aadhaar based authentication.

Table 92: End point layer controls

8.2.7.5 Application Layer

To ensure the smooth running of the production set-up, maintaining a separate development, testing and staging environment is recommended.

1. The technology selection should be done to help to provide better security along with the performance.

Every application should go through vulnerability assessment and penetration testing before making it available in the production setup. VAPT is carried out by the CCA empaneled agencies. VAPT should be carried out at a regular interval and whenever any new patch or functionality is added or removed from the service/application.

8.2.7.5.1 Functionality at Application Layer

Below functionalities should be provided at the application layer to secure the service/application and its data:

1. Static testing and code review - The purpose of this type of testing is to identify the vulnerabilities without carrying out the actual execution of the code. The development or implementation team does this testing and provides the reports related to the same.

2. Dynamic application testing- The purpose of dynamic application testing is to determine the associated security vulnerabilities in the code by executing it. This helps to identify the security issues related to the complete production set-up including the exact version of the application and application stack.

3. Web application firewall: Firewalls at the application level should be given consideration to prevent the attacks such as SQL injection, Cross-Site Scripting (XSS), cross-site request forgery etc.

4. Vulnerability assessment and penetration testing: The objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation. A policy should be defined by the departments to foresee the possible vulnerabilities and simulation of exploiting those vulnerabilities. The policy should address the guidelines VAPT at regular intervals should be carried out to exploit the vulnerabilities associated with configuration changes at various levels, i.e., network, application server, database servers etc. Vulnerabilities assessment should also be carried out w.r.t possibility of execution of malware, viruses etc. and should be defined in the policy.

5. User Authentication: There should be a proper authentication mechanism being implemented in the applications for providing access to sensitive information to the users.

6. Database monitoring- Monitoring the application, database servers for their uptime, threats which are being observed

7. Role/ Rule-based access: A proper authorization policy and rules should be defined to prevent unauthorized access to the various areas of the application.

8.2.7.5.2 Controls at Application Layer

1. Applications should not be made public unless and until tested for security.

2. A regular audit should be conducted of the application/service.

3. Avoid unwanted access.

8.2.7.5.3 User Authentication:

Users should be authenticated with a strong authentication factor based on the sensitivity of the application/service as well as data.

Application Access Control / User Access Management

	Objective: To ensure authentic access to the systems and services/applications.	
1.	Registration and Deregistration	Only authorized users should be allowed to access systems and services. In order to identify the authorized users, a facility of registration and de-registration should be provided for every service. This will help enable the appropriate access rights.
2.	Access Provisioning	A formal access provisioning of the users should be implemented. It will assign or revoke the access rights for the users.
3.	Authentication Mechanism	Appropriate authentication mechanisms such as password, OTP, Digital Certificate, PKI, Biometrics should be implemented for providing the access to the services. That access can be controlled based upon the data and service sensitivity and in accordance with the security policy of the state/organization/department.
4.	Secured Log-in process	Every service/ application can be accessed only through the secured log-in mechanism based on the chosen authentication mechanism as per the policy of the state/organization/department.
5.	Password Management	Password management systems should be interactive and should ensure quality passwords. The password management systems should also be secured and should have a provision such that no password can be leaked.
6.	CAPTCHA Management	reCAPTCHA version which shall be used in the project shall not have any user interaction. It shall be just behavioral analysis, so there is a frictionless user experience and enables reCAPTCHA to better detect fraud by comparing all manner of transaction behavior. The supplied version of reCAPTCHA should allow integration with an API-based service, should have SLA/SLO so that it doesn't become a bottleneck while the customer is trying to do different transactions on the portal.
7.	Access control to source code of the program	Access to program source code should be restricted.

| 8. | Management of Secret authentication information of the users | Secret authentication information of the users should be managed as per the state/organization or national policy. The information storage should comply with the acts related to storing the secret information of the user. |

Table 93: User authentication controls

8.2.7.5.4 Authorize:

Though the user is authenticated, she/he may not be authorized to access certain systems, data, information, services. Every information and information providing facility should be accessed only by its authorized users.

The access rights usually are time-bound and should be verified on a timely basis to avoid unauthorized access. The change in the business processes should immediately reflect in the authorization policy and be implemented on priority to avoid unwanted access. For implementing authorization along with multi-factor authentication rule or role-based access should be provided to the users.

8.2.7.5.5 Logging and Monitoring:

Objective: To record events to create evidence.		
1.	Log creation	Events such as user activities, failures, exceptions, information security events, server, firewall, IT equipment transactions etc. should be recorded and maintained in the log format. System administrator, system operator activities also should be logged and protected.
2.	Protecting logged information	These log files are important evidence and should be maintained and also secured from hacking. An encryption mechanism can be used to protect log files from unauthorized access and tampering.
3.	Clock synchronization	The reference point for all the activities, events, logging is time and hence the clocks of all the relevant systems should be synchronized.

Table 94: Authorization controls

8.2.7.6 API Security

It is possible to attack or leak the data in transit while calling the API and hence the API design is equally crucial when talking about security. Following care must be taken while designing API:

1. Information required for routing or interpreting the contents of the packet should be part of the header and should be appropriately tagged.

2. The body of the packet should be encrypted and should not be easily accessible. The user's personal identity information should be part of the body of the packet and not the header.

3. Provide some default value for optional parameters/ tags.

4. Only necessary information should be taken from the user and unnecessary information exchange should be avoided.

5. Preferably no personal information should be shared as a part of the response.

6. API should be made available only on the secured channel.

7. Access to API should be provided only to authorized users.

8. Whenever data is exchanged between two servers, it should be done only after proper white-listing of the IPs; requests should not be accepted from any other IPs.

9. Mobile apps which are open to the public are particularly vulnerable. Sensitive or personally identifiable information should not be shared through such apps as the authenticity of the end-user is questionable and also because mobile apps can be easily reverse engineered to retrieve the tokens etc. which are used to communicate with the server. Aadhaar APIs can be considered as a reference for designing secured APIs.

8.2.7.7 Data Layer

Data is the most crucial aspect of security and should be protected in multiple ways. Classify the data as per its sensitivity level (Highly sensitive, medium sensitivity, not very sensitive). Appropriate methods should be chosen while storing the data in the database, files, directories or any other mechanism. Based on the level of sensitivity the policy should be chosen for storing the data. Various mechanisms can be encryption, hashing, maintaining in clear text format. The storage location is also dependent on the sensitivity of the data.

Access to any of the data should be provided through APIs or through proper authentication and authorization. The transport of data on various channels also should be ensured for security.

8.2.7.7.1 Functionality at Data Layer

1. Data needs to be secured when at rest, at motion i.e., in transit or in use – Every piece of data irrespective of its sensitiveness need to be secured against the threats of unauthorized access, data corruption or complete data loss Depending on the sensitivity and availability needs, methods should be applied to secure the data.

2. Identity and access management for data – The data should be accessible to only authorized persons, at the appropriate time and only for the specified purpose.

3. Access Right Management – Access to data should be restricted by creating and applying a policy for every kind of data set. Data access policy will define the constraint for controlling the data access by its users. It will help in applying appropriate read, write controls over data elements.

4. Data Integrity monitoring – Data Integrity is as important as any other aspect of data security. If the correctness of data cannot be determined, it is almost the same as data loss. In some cases, having data with compromised integrity is more dangerous than having no data. Therefore, a mechanism needs to be applied to monitoring data integrity at various stages to enhance authenticity, reliability and availability of data.

The requirement results in the appropriate access control for data. Regular monitoring, logging, auditing of data is required. A backup plan should be prepared and implementation as per the plan should be ensured. GeM data backup policy should be considered while defining the data backup policy for the application or service.

Data should be classified as per its sensitivity and the appropriate rights should be imposed for the modification of the data.

8.2.7.7.2 Controls at Data Layer

Backup:

Objective: To protect data against data loss.		
1.	Policy Creation	A backup policy should be created and documented to create the backup of the data, information, system and software.
2.	Information Backup	Regular backup should be scheduled for applications, systems, information and data as per the backup policy. The backup should be tested regularly to verify its integrity.

3.	Back up protection	Backups should also be maintained in the encrypted format to protect its integrity.

Table 95: Data layer controls

8.2.7.7.3 Personally identifiable information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories and websites. Sensitive PII is information that, when disclosed, could result in harm to the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Aadhaar numbers.

PII data will require multiple layers of protection including but not limited to encryption, masking, anonymizing, pseudonymizing.

8.2.7.8 Security Standards

1. ISO/IEC 27001:2013, ISO/IEC 27002 are referred for defining the control objectives and controls. These standards are followed in the organization for defining, implementing and monitoring information security at various levels. The standard elaborates on the controls at management, user access control, key management and cryptography, human resource management, system and application access etc. It is best practice to follow the controls given in these standards to ensure information security in systems, applications and information facilitating assets in the organization.

2. ISO/IEC 27002 is referred to as a guideline while designing this document. The standard also provides guidelines to design controls for organization-specific security requirements.

3. NIST SP 800- 30 is referred for defining risk assessment and risk management.

4. Cloud Security Standards by cloud standards customer council is referred for providing suggestions regarding controls for cloud environment

8.2.8 Application layer

The Application layer should comprise of 4 essential sub-components:
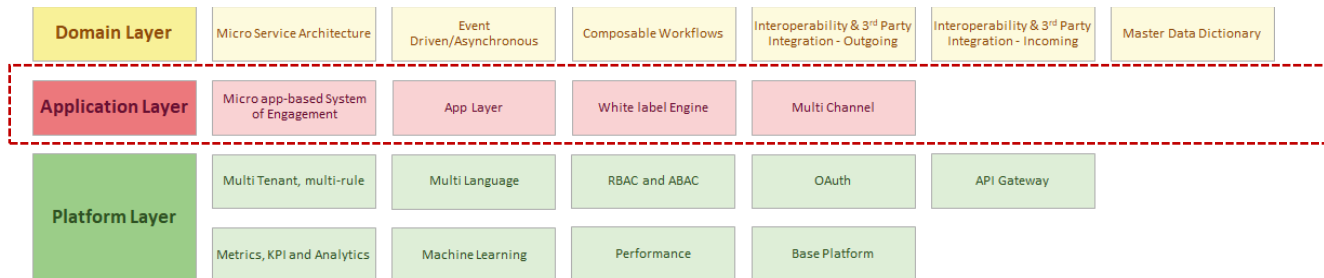
Figure 59: Application layer of target state platform architecture for GeM

Microservices provide a great way to increase cohesion and loose coupling, the client layer is also becoming benefit from such architecture. There are 2 main components of application layer:

1. **Micro Front – end architecture layer:**

   a. The architecture of the Application Layer will be designed using a micro-apps strategy.

   b. Micro apps should be compatible and flexible to be evolved without dependency on other apps simultaneously should maintain the system consistency and user experience.

   c. Usage of modern web framework to define client layer adhering to micro frontend architecture and to avoid tight dependency bet ween parent – child component. Popular frameworks which are available in the market - Angular, React, Vue.

   d. Data sharing between micro apps should be separated to a shareable data layer through query params, browser storage capability like session-storage, cookies, or indexed DB to store complex data structure.

   e. Compatibility to be maintained between various apps, so that micro-apps can be evolved without being dependent on other apps and not break overall system consistency or break user experience.

   f. The target architecture should adhere best practice via workspace, projects and libraries

g. Design of complex web app to be build using micro frontend by splitting based on feature or domain

h. Separate codebase for each micro frontend under CI-CD pipeline

i. Micro frontend apps should be bundled and served together web app shell.

6. **Micro-app layer :**

a. App layer should ensure application specific business logic, and data shaping needs are not force-fitted into the micro-services layer.

b. Micro-services layer should remain truly reusable and driven by the domain model / business architecture

c. All the app specific customization to a domain model properties influenced by screen design to be extracted from domain logic to app-specific layer.

d. App specific services layer is expected to provide the necessary decoupling in the architecture.

e. App layer should also provide the customization configuration need for presentation layer such as mandatory and optional form validation rules, visibility of fields based on use case or tenant needs.

f. The application layer should have white-labelling support.

g. The design should provide flexibility in configuring the application layer look and feel. The configuration would include UI themes, fonts, font-sizes, colors, logos and the likes.

h. Application layer should be modular enough so that code customizations be feasible by individual states to make those UI level changes that may not be possible via code configuration

i. White label engine should support for server driven i18n capability for app labels, success and error messages

j. With incorporation of white label service, it would be possible to change the look and feel, app linguistic without the need of deployment.

k. There should be a default value for all configuration present in client layer which

are being fetched from white-label service to mitigate fallback in case of missing any value in server.

l. Platform needs to support business through multiple channels such as Web, mobile.

m. Target platform should be built from API first approach ensuring same set of endpoints exposed by services can be consumed by different channels.

n. Platform should have capability to track channel for any transactional data present in the system.

o. Mobile Device Management functionalities to be provided by MSP for effective mobile application experience management.

8.2.9 Platform layer

The Platform layer should comprise of 9 essential sub-components:
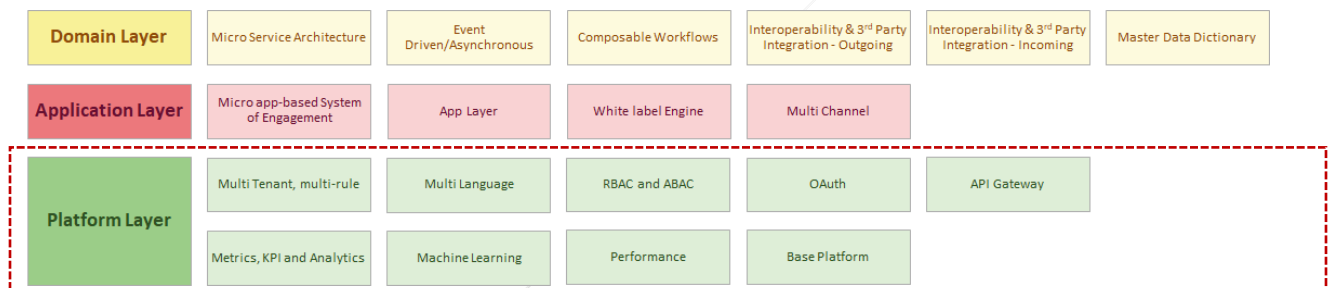
Figure 61: Platform layer of target state platform architecture for GeM

Multi-tenant, Multi rule:

1. Platform should possess multi-tenancy, where each state will be an independent tenant

2. Each state may have different procurement rules, and to that extent the platform design will need to provide for tenant specific rules.

3. The rules should be data driven to the extent possible, however, not all requirements for rules customization can be fulfilled via data configuration.

4. The platform design needs to allow for simple code extensions / plugins where state specific rule can be coded if needed

5. The target architecture should support multi-tenancy using separate database for each tenant model. The connection parameter for different database instance can be configured in central tenant registry which stores all the meta info of the tenant.

6. The architecture should ensure connection parameter for different database instance to be configured in central tenant registry which stores all the meta info of the tenant.

Multi language:

1. Platform needs to support multi-language capabilities and bi-lingual (English and Hindi) search capability. MSP shall be responsible for translation of content in multiple languages and updation of the same on the portal. Languages supported should be at least English, Hindi, Assamese, Bengali, Gujarati, Marathi, Kannada, Malayalam, Telugu, Odia, Punjabi, and Tamil.

2. Multi-Lang needs to be provided not just for static UI labels, but for data as well. For example, translate the word "Product" on the UI. to store and fetch Product Name, Product Description, and Product Specification in multiple languages.

3. Target platform should model multi-lingual capability such that it can support N languages and adding a new language should not have any technical complexity.

RBAC and ABAC features:

1. System should implement role-based access control.

2. Roles should be externalized from the services - It should be possible to create new roles using data configuration and give relevant rights to the role also using data configuration

3. System should also implement attribute-based access control. For example, a bid creator should be able to access only the bid created by them, with permissions to execute the "get-bid-by-id" service endpoint.

4. Systemic controls also should not be hard coded in the services, but be implemented via interfaces / service extension code

5. All the endpoints exposed by a micro-service or a consumer listening to an event should be controlled by a defined authority to implement role-based authorization.

6. Role should be defined based on set of authorities and should be validated by a policy evaluator mechanism.

7. Authorization system should be robust enough to add/revoke any end-point access without a need of deployment.

OAuth features:

Security being most crucial part of the system should be dealt with utmost care.

1. PKCE, an extension to Authorization code Flow should be used in the OAuth2.0 authorization framework. PKCE would protect the client secret storage in SPA which is risky and can be compromised.

2. SSO and OAuth should be implemented by separate authorization server.

3. A well-defined and tested tools like KeyCloak or any IAM provider should be used.

4. Identity service should have dynamic token-based communication with state information

5. Service should ideally verify the information in the JWT token verification. Reverse proxy-based token verification would provide external users to have a first pass on the reverse proxies

6. Identity and access management platform should in turn provide resource information for each service resources.

Implications of zero trust environment should be considered as guidelines for target architecture

Metrics, KPI and Analytics features:

1. The platform needs to have a solid BI and analytics framework. In order to provide robust way of making data driven business decisions, cross functional workflows and to establish growth metrices across the time frame

2. Based on the domain model and business architecture, processes and KPIs for the processes need to be identified.

3. Thresholds and targets need to be set for KPIs and metrics.

4. Appropriate data modelling needs to happen to calculate and capture summaries incrementally and provide high performant reports

5. Analytical reports should not be run off OLTP schemas and hence a separate read only schema should be configured known OLAP.

6. Data synchronization should be done through ETL, events from OLTP to OLAP

7. The data model for OLAP should be flat schema as far as possible for faster querying without bearing the cost of JOINS (in case of RDBMS).

8. Proper dimensional model design with proper facts, dimension, attributes, fact table, dimension table for BI attributes.

Machine Learning:

1. Platform should be capable of deploying machine learning algorithms in order to discover and spot deviant patterns like by passing of procurement rule by Buyers or Sellers.

2. System should perform predictive modelling ,using base knowledge, for which the answer is known. The knowledge should enable (trains) the system to learn and perform predictive modelling for e.g., frequently bought product data history would propagate the model to propose users to buy a particular product category

3. Predictive modelling would be performed based on time series regressions or using supervised/unsupervised learning techniques in the system

Performance:

1. Effective performance using infrastructure as a code in order to provision new resources in case of high load transactions.

2. Performance engineering should be adopted as a methodology at various steps:

   a. Logging of queries to database server, their execution time while development to identify slow traces and poor performing queries.

   b. Performance testing using tools like Apache JMeter to measure the load threshold of service under fully loaded DB and empty DB.

   c. Presence of Infrastructure as Code automation to provision resources automatically when load increase and services require more computational resource.

Base platform:

1. The platform needs to provide a set of base libraries that enforce such cross-cutting concerns on the service / data table in question so that impact of human error in coding is minimized

2. Definition of audit fields across the entities, common models, endpoints which might be required by all domain should be a part of platform-base and it should be available to all microservice via a dependency.

3. Definition of data archival design as per the archival policy(hot, warm and cold storage)

4. The target platform should support multiple service-base for different domain service requiring different scheme of database such as RDBMS, Object database, NoSQL database or graph database based on requirement.

8.2.10 Enterprise Architecture Governance

The Objectives of the EA Governance are

1. To ensure the effective introduction, implementation, and evolution of architectures within the organization;

2. To ensure compliance with internal and external standards and regulatory obligations;

3. To establish processes that support the fulfilment of the above objectives

4. To develop practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

MSP should facilitate and participate in setting up joint Enterprise Architecture governance along with GeM- following the indicative below structure. The detailed plan for the same should be submitted by MSP in the technical proposal
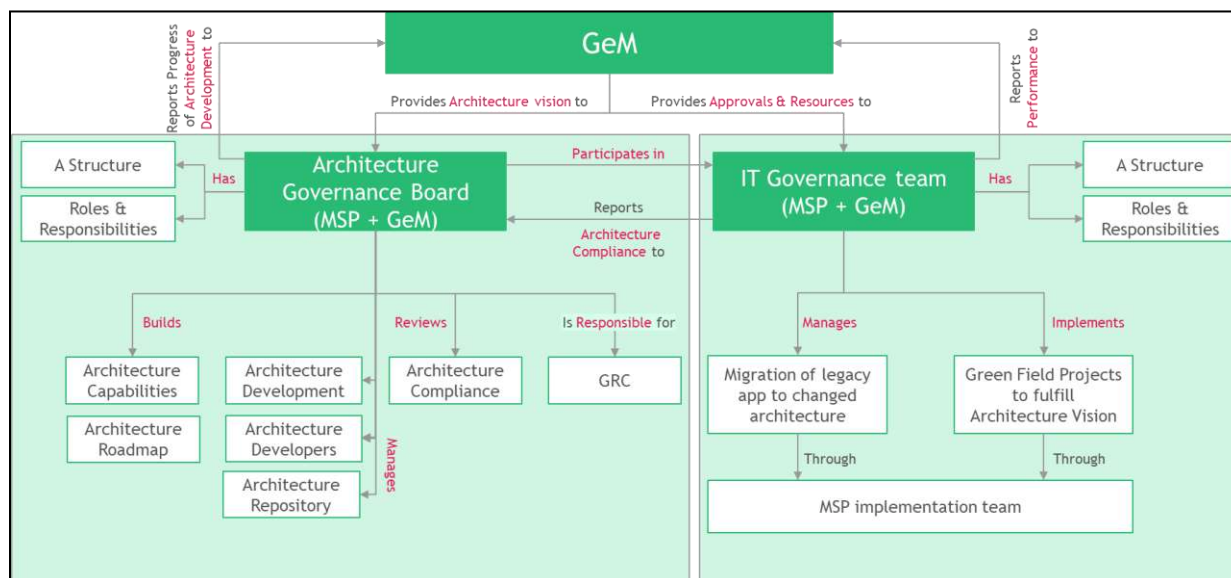
Figure 60: Architecture governance structure

8.2.11 Solution Component

It is preferable to deploy open-source solutions to build GeM new system, which is modular, scalable, and portable across platforms. All the platforms and solutions proposed for GeM system should be vendor neutral and GeM can replace any platform without any constraint.

An indicative list of solution component has been provided below. The Solution Components in the list have been identified as Core and Non-Core. For each solution component, the requirement in terms of Open Source / Bespoke / Proprietary is also given in the table below. Enterprise support, from respective OEMs, is required in India for all the solution components mentioned in below table, as applicable.

Solution Component	Type	Type of component (Open Source/ Bespoke**/ Proprietary)
Operating System	Core	Open-Source product
Web Portal	Core	Bespoke/ Open-Source product
Mobile Solution	Core	Bespoke/ Open-Source product
Web Server	Core	Open-Source product

Application Server	Core	Open-Source product
e-Commerce engine	Core	Bespoke/ Open-Source product
e-Procurement complete system including e-Tendering	Core	Any of the below can be used: ▪ Open-Source product-based solution which has to be made compliant to STQC guidelines by MSP for later certification ▪ STQC certified/ compliant e- Procurement Complete System including e-Tendering
Learning management	Core	Bespoke/ Open-Source product
Grievance Management	Core	Bespoke/ Open-Source product
Workflow Management	Core	Bespoke/ Open-Source product
Rule Engine	Core	Bespoke/ Open-Source product
Queue-based Messaging	Core	Open-Source product
Document/ Content management	Core	Open-Source product
Master data management (MDM)	Core	Open-Source product
RDBMS/non-RDBMS	Core	Open-Source product
MIS Reporting	Core	Open-Source product
BI Tool	Non- Core	Open-Source product/ Proprietary
Analytics Tool	Non- Core	Open-Source product/ Proprietary
ETL	Non- Core	Open-Source product/ Proprietary
API Gateway	Core	Open-Source product
Event stream engine	Core	Proprietary
Containerized infra	Core	Open-source product
In Memory-Caching	Core	Open-Source product

CRM	Core	Open-Source product
Chatbot	Core	Open-Source product/ Proprietary
Build Management	Core	Open-Source product
Source Control	Core	Open-Source product

Table 96: Solution Components

All *non-core components should adhere to the architectural principle.*

** Any bespoke development must be done on an open-source programming language.

It should be noted the selected MSP will be responsible for the overall support and maintenance of the GeM solution till the end of the O&M phase.

8.2.12 APPENDIX I: Current Technology Stack
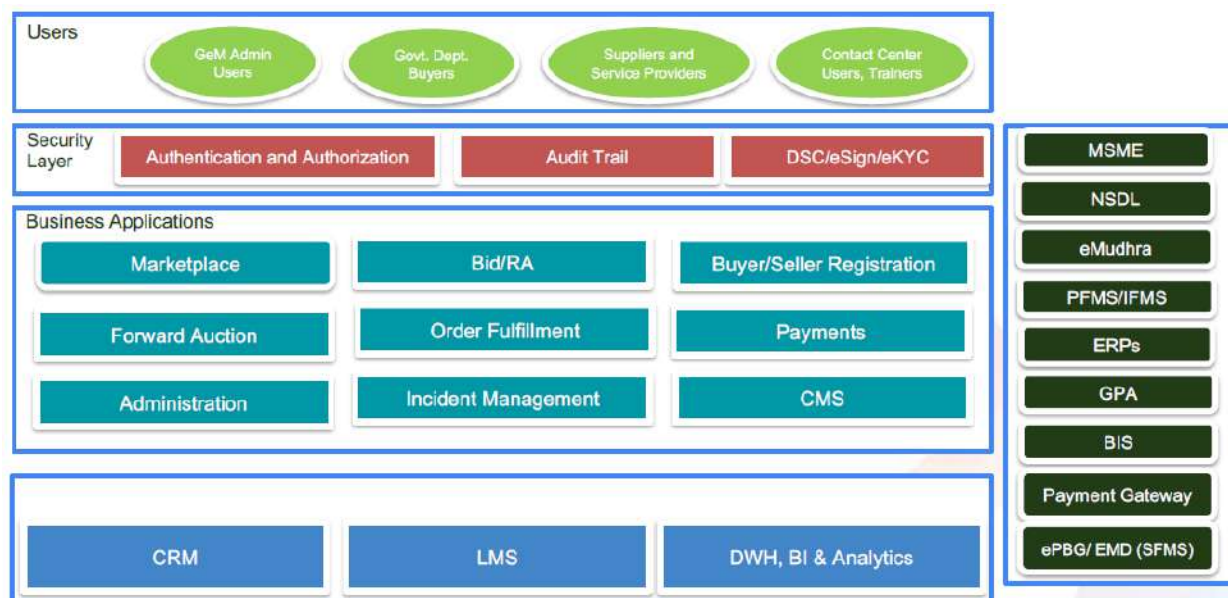
Figure 61: GeM's current application landscape
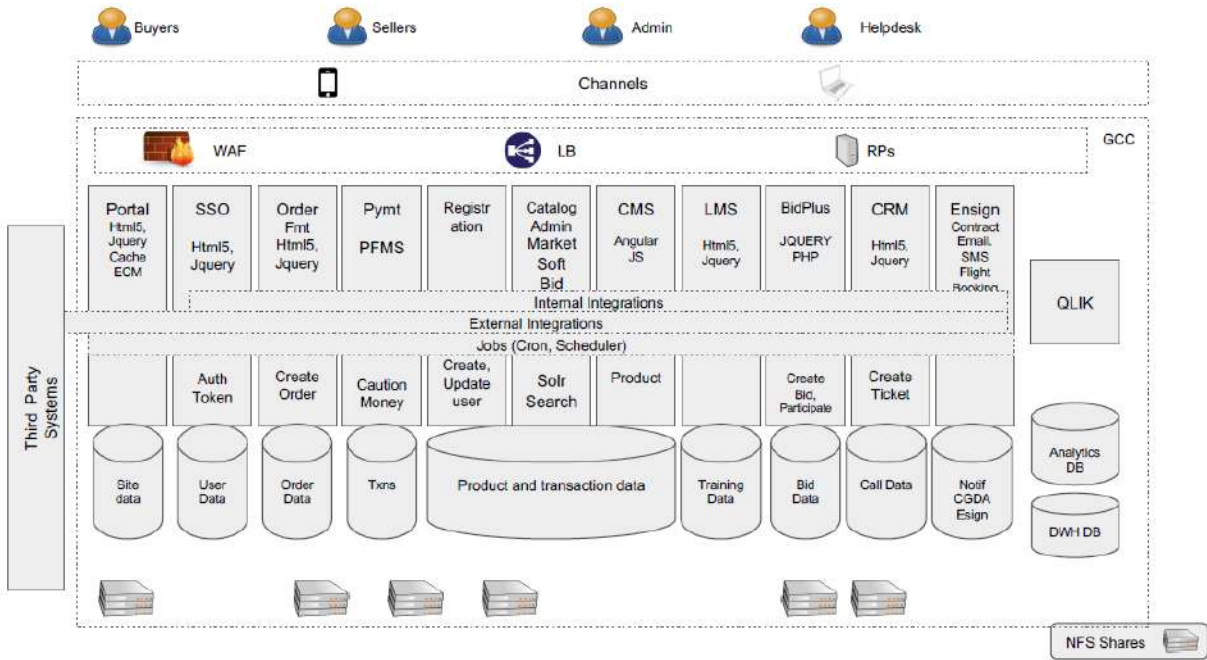
Figure 62: GeM's current micro-services interactions
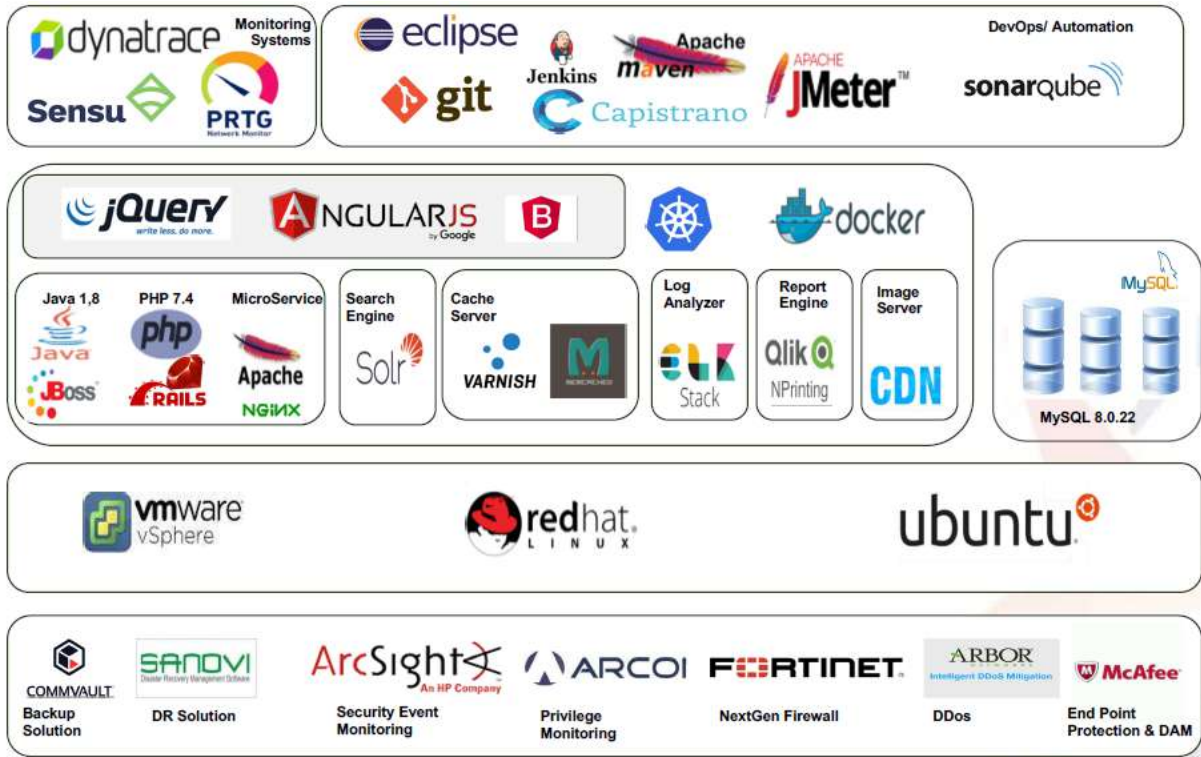
Figure 63: GeM's current technology stack

8.2.13 APPENDIX II: Current Platform – Architecture & Design

This section provides an indicative view of the current GeM Platform's architecture and design. Multiple enhancements and modifications have been done to the current GeM platform since its inception. Hence, as mentioned in Section 3.1.2 of Volume 1 of the RFP, the incoming MSP must perform a detailed assessment of the business and IT solution requirements as mentioned in this RFP. Additionally, the MSP is required to carry out exhaustive requirements gathering exercises with the GeM team, including but not limited to review of existing code, BRDs and other documentation, for understanding and drafting the requirements.

8.2.13.1   Application architecture
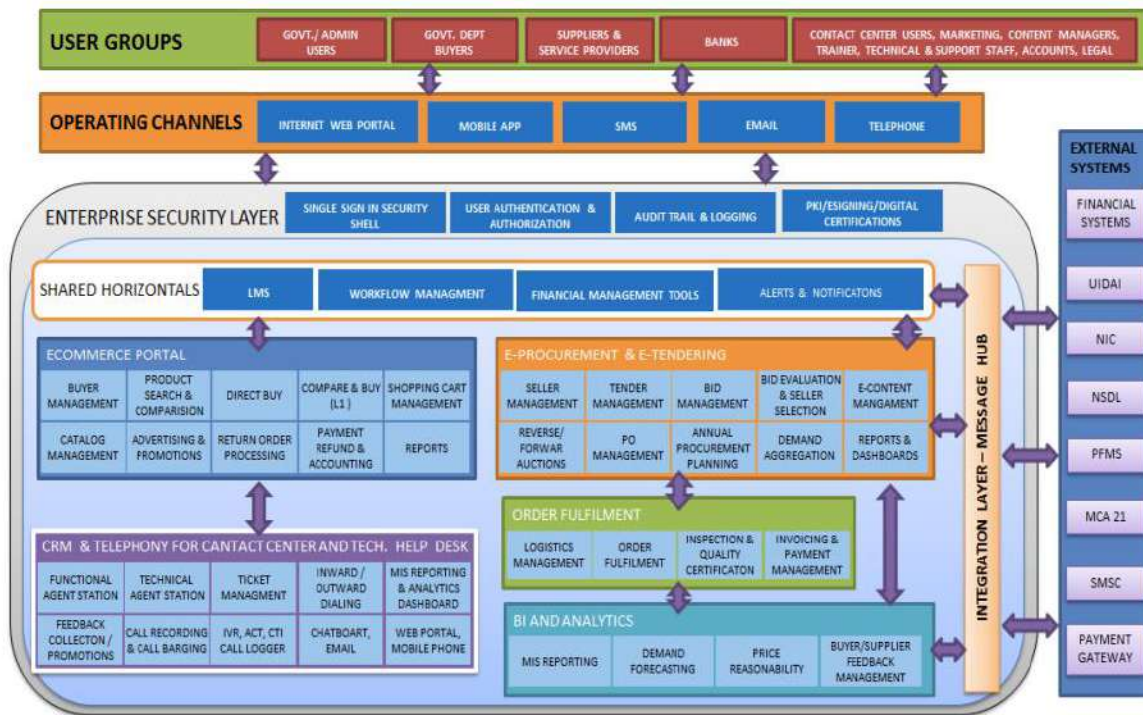
Figure 64: Application architecture

Multiple software layers are involved in the design of GeM portal. The full portal is made up of 3 major interfaces:

1. Internal software interfaces

2. External software interfaces

3. Communication interfaces

Internal software interfaces:

 a. Internal communication happens via micro services. Each sub-portal e.g. market, bid and fulfilment pass important data by the mode of micro services.

b. Single sign on – ARX – User management at backend is maintained at central location and every sub-portal uses the same SSO to login in their respective application.

c. Common services are present to send Email and SMS.

Remarks: Presence of Spaghetti codes and tightly couples services in the current system.

External software interfaces:

External communication happens via central message hub integrator. All the 3rd party integrations are done via a central hub to keep the interaction secure and uniform.

a. Aadhaar

b. PAN

c. MCA

d. GSTN

e. SMS & Email

f. PFMS

g. E-sign & DSC

h. TRIFED & SHG

i. NIC LDAP

j. Weavers/Artisan

The **central payment hub** is integrated with:

d. GPA / SGPA

e. IFMS

f. ERP

g. TreDS

h. PFMS

i. Payment Gateways

8.2.13.2   Communication Interfaces

In GeM primary communication is done over https portal. Following methods have been added wherever appropriate:

a. SMS: order creation, promotion, order notifications, Payment notification

b. Email: order creation, promotion, order notifications

c. https: Portal access, Mobile Website

d. IVR: Contact center

8.2.13.3   Architecture Design Principles

This section defines architecture principles that were followed in development of the current GeM platform.

8.2.13.3.1   Service Modularity

The Services are designed in such a way that they are deployed independently and hence are scaled up individually based on business needs. These Services are designed on Micro-service architecture (SOA) for high-performance scalable solution with extensive use of open source software and Cross platform/Interoperability support.

Remarks: While micro-services have been deployed in pockets, core modules continue to be monolithic. Communication between core modules services such as e-Marketplace and order tracking & invoicing happens via point to point RESTful APIs.

8.2.13.3.2   Layered Architecture

Built Architecture is layered architecture wherein the presentation layer is loosely coupled with the services layer and the services layer is in turn loosely coupled with the data layer. With this design,

the solution has the flexibility to deploy them separately and ensure that there is no single point of failure. This also enables differential scaling of a component in one layer to meet specific workload requirements.

Remarks: Architecture is not entirely loosely coupled as it has MVC framework making horizontal scaling challenging.

8.2.13.3.3   Scalability

The components are built on SOA principles, and each component in turn is scaled horizontally to handle changing workloads. The components have scaled out horizontally and handle future volume spurts by adding additional compute without any perceptible degradation of performance or SLA breaches.

Remarks: GeM System is scaled vertically. Horizontal scaling is done manually via infrastructure provider.

8.2.13.3.4   External Service Interfacing

All the interfacing with external (3rd Parties) Services is via API (Integrator). Following principles are followed:

1. Faceless API based web services are used to communicate real time and synchronously for high security connectivity or where the data payload is heavy

2. REST APIs are used for real time connectivity for inter Service connectivity and connections to government Services,

3. Messaging is used for real-time asynchronous communications typically for feeds/notifications/data replication

4. File upload (ETL like function) is used to extract and mash up data from various sources to create a logically connected data dictionary. Similarly, data extracts are generated for asynchronous batch based data feeds to be sent to connecting Services.

Remarks: Distinction of external and internal requests not supported by API gateways while doing queue management.

8.2.13.3.5   API Based Service

The GeM Service has been built as a faceless Service with API driven architecture at the core of it. GeM portal is one such application on top of these APIs.

8.2.13.4   Micro-services architecture

For optimum usage of the underlying platform, MicroService pattern is used at the service layer to carefully handle business requests, initiated by GeM users.

MicroService architecture pattern allows, designing highly scalable e-MarketPlace to achieve high performance. Since the number of concurrent users in GeM increases gradually, application servers at DC & DR are scaled up.

Remarks: While micro-services have been deployed in pockets, core modules continue to be monolithic. Communication between core modules services such as e-Marketplace and order tracking & invoicing happens via point to point RESTful APIs.
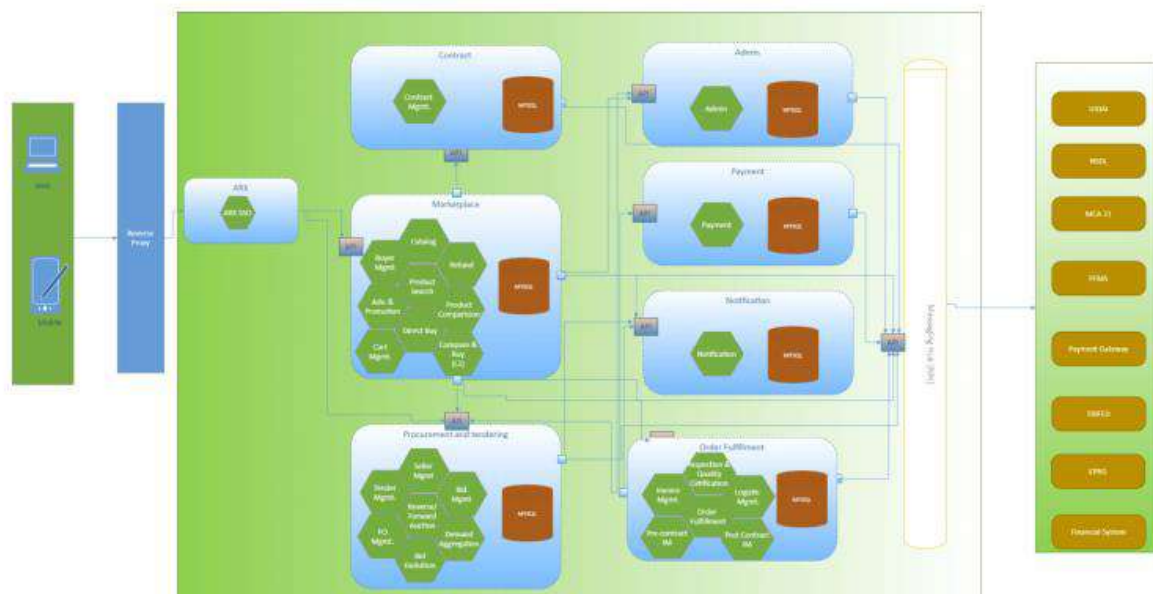
Figure 65: Micro-services architecture

8.2.13.5 Technical Architecture

The GeM core platform follows Microservice Architecture and exposes the business services via an API Layer. For all service communication, both internal and external, the only gateway to the service is its API.
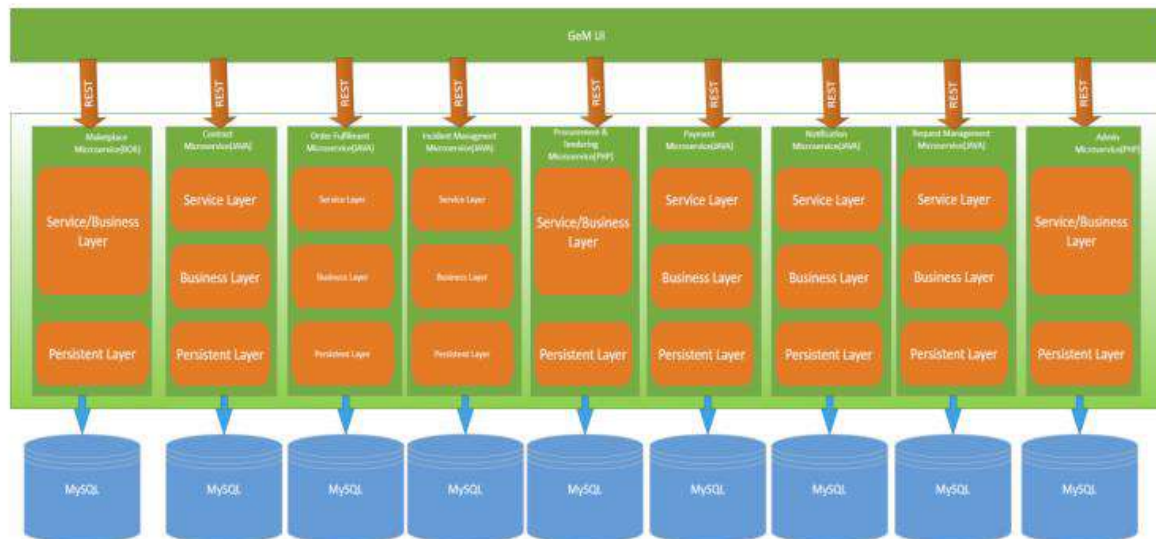
Figure 66: Technical Architecture

Each Microservices Layer allows for a modular architecture of the services providing horizontal scalability as the service load demands. The API Layer centralizes and unifies functionality in one place, so it is easy to add, remove and reconfigure services in a uniform way. The APIs are Restful, JSON, and/or XML. Endpoints have been shielded from direct interaction with the internet

The API Layer provides the following:

1. **Authentication (Basic, OAuth):** Provides authentication layer for all API calls via multiple configurable mechanisms. For advanced authentication needs, integration is done with standalone authentication.

2. **Security (SSL, ACL, CORS, IP (White list/Black list)):** Access control mechanisms for all APIs providing additional security layers like SSL.

3. **Traffic Control (Rate & Response Rate Limiting, Request Size Limiting):** It manages, throttles and restricts inbound and outbound API traffic. More specifically, architecture limits how many HTTP requests are from a certain consumer, blocks malicious requests configurable on the request or on the response.

4. **Transformations**: (Request & Response Transformers): Request transformation has been added before hitting the upstream server or response transformations, before returning to the client. Also, each request/response is correlated via a unique ID. This is used in creating audit trails.

5. **Logging:** Log requests and response data is integrated into the central logging Service. Also supports logging to other endpoints via different protocols.

Remark: While micro-services have been deployed in pockets, core modules continue to be monolithic. Communication between core modules services such as e-Marketplace and order tracking & invoicing happens via point to point RESTful APIs. All the platforms are indexed to a single MySQL database with absence of DAO (Data Access Object).

8.2.13.5.1 Technology Services

This section describes major services with choice of technology stack.

1. **Application Service**

   The buyer service is built on Ruby on Rails. Ruby on Rails uses the Model-View Controller (MVC) architectural pattern in order to improve the maintainability of the application. The MVC allows a clean separation of concerns, in the way that it keeps the business logic separated from HTML views.

   The Rails engine uses a process model i.e. each process handles only one request at a time. Tendering service is built on PHP CodeIgniter Framework. It uses the Model-View Controller (MVC) architectural pattern in order to improve the maintainability of the application. The MVC allows a clean separation of concerns, in the way that it keeps the business logic separated from HTML views.

   Order Fulfilment and Contract Mgmt. services are built on the Canvas framework. Canvas is a rapid application development framework with a rich library of client side java components and full wiring to the server side components.

   Canvas internally uses MVC architectural pattern for clear separation of concerns in the way that it keeps the business logic separated from HTML views. Fulfilment service is integrated with internal (Market place, Admin (Admin panel), ARX (SSO authentication), BI (for data analytics and dashboard), Notifications (for alerts) and Contract management (for Contract pdf generation), and external services (e-Mudra (E sign), NIC for SMTP/SMS).

2. **Search Service**

Search service is implemented using the Solr Cloud framework. Solr is highly reliable, scalable and fault tolerant, providing distributed indexing, replication and load-balanced querying, automated failover and recovery, centralized configuration and more. Apache Solr includes the ability to set up a cluster of Solr servers that combines fault tolerance and high availability.

Remarks: Solr is being used as a caching platform. Complex queries are not supported through Solr.

3. **Database Service**

Database service is built on the open source flavour of MySQL DB. Each SOA component has its own DB schema making sure that performance/scaling needs can be fine-tuned. Each DB server has enough memory to make sure that the working data set is served from memory. This ensures that the queries have least SLA.

4. **Caching Service**

MemCached has been the best selection for caching as it is an in-memory key-value store for small chunks of arbitrary data (strings, objects) from results of database calls, API calls, or page rendering.

5. **Business Rule Engine:** Currently Drools is used by the marketplace as a rule engine.

8.2.13.6   Database Architecture

The following is the Database Architecture for GeM:

MySQL InnoDB has been used as a database server for the application components. In GeM, multiple primaries have been adopted to ensure high availability is achieved.

MySQL InnoDB Cluster has proven with the first GA release its potential as the native out-of-the-box HA solution for MySQL.

With the second GA release, usability, stability and flexibility have been greatly improved, Client applications are connected to the ports that MySQL Router provides, without any need to be aware of the InnoDB cluster topology.

In the event of an unexpected failure, the InnoDB cluster adjusts itself automatically and MySQL Router detects the change. This removes the need for client application to handle failover.
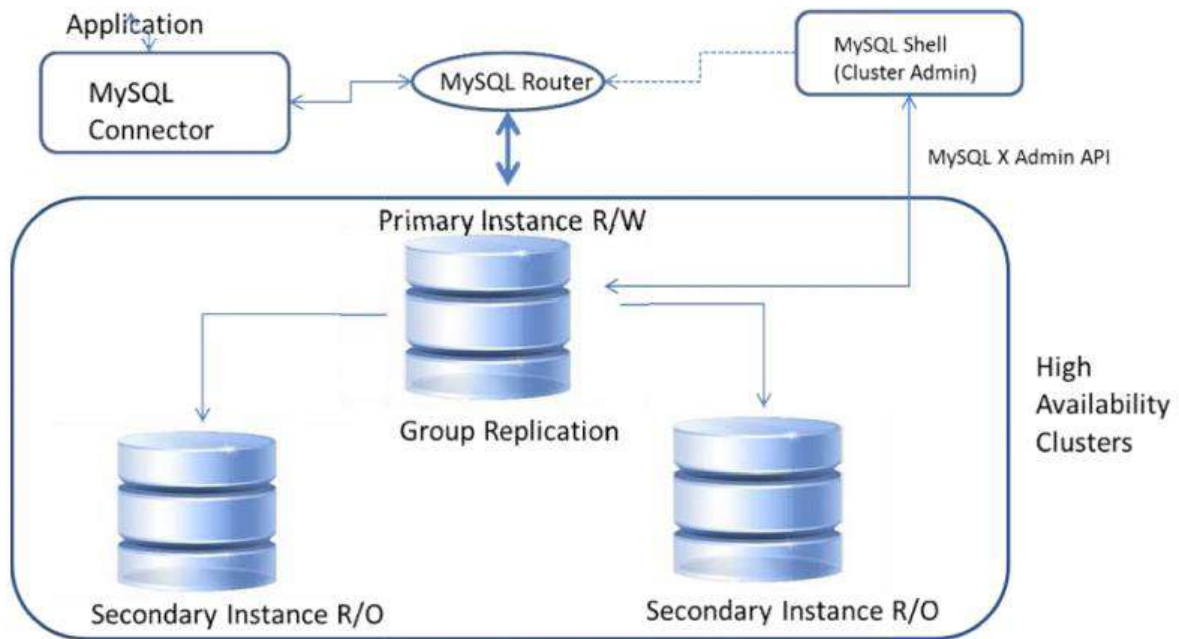
Figure 67: Database Architecture

8.2.13.7   Deployment Architecture

The solution design and deployment architecture ensures that the application is deployed in a centralized environment offering Service High Availability and failover.

The solution meets the following availability requirements:

1. Load Balanced across two or more Web Server avoiding single point of failure.

2. Deployment of multiple application instances is possible.

3. Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.

Remarks: GeM's deployment architecture involves manually managed CI and a semi-automated CD.
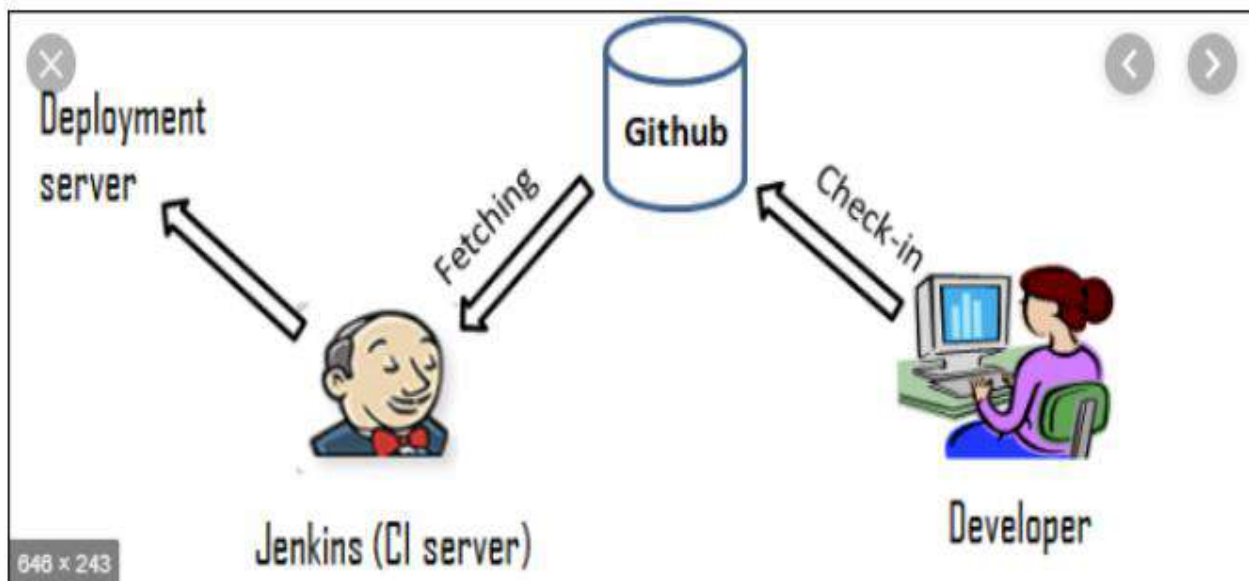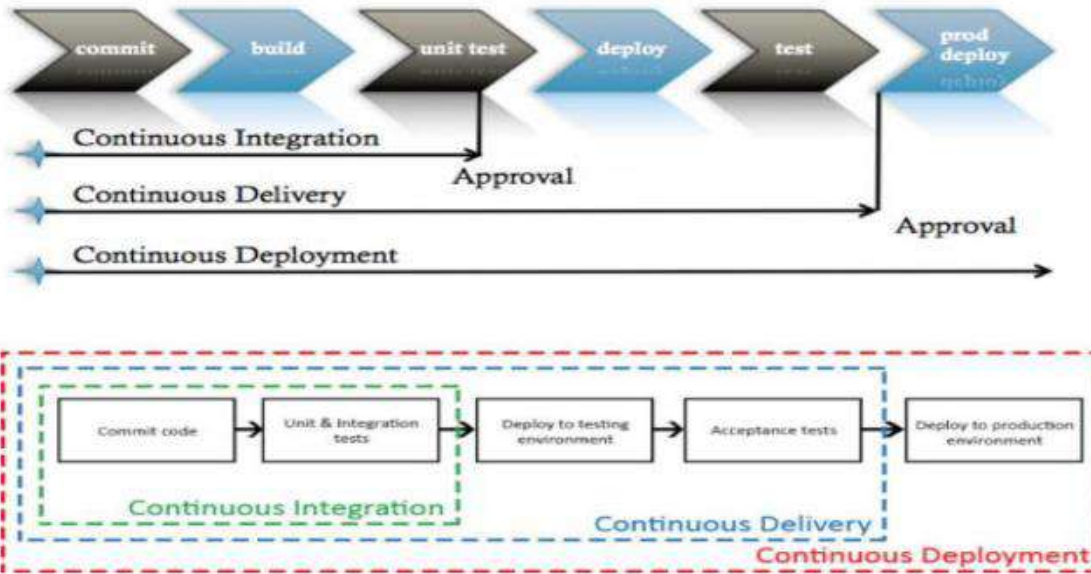
Figure 68: Deployment Architecture

8.3 Annexure C - Cloud Service Requirements

8.3.1 General Requirements

#	Details
1	The MSP should architect an Infrastructure as a Service (IaaS)/ leverage Cloud Service provider's Platform as a Service (PaaS) offering as suitable on Virtual Private Cloud (VPC) /Government Community Cloud (GCC) deployment model (As per MeitY), or any other deployment model as instructed by GeM, of a MeitY Empaneled Cloud Service Provider. In the case of the GCC model also, the GeM application and infrastructure stack should be logically segregated from the other Government clients.
2	MSP shall assess the infrastructure requirements (including OS Instances, Storage, Networking, Security, etc.) for hosting and maintaining all required applications/services. The MSP shall provide the services in conformance with the SLAs as described in this RFP.
3	The MSP should ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
4	GeM will not be responsible if the MSP has not provisioned some components, sub-components, assemblies, and sub-assemblies as part of the bill of material in the bid. The MSP will have to provide the same to meet the solution requirements at no additional cost and time implications to GeM.
5	The Virtual Private Cloud/GCC services of the MSP should be available on a pay as per usage model and Fixed-Billing model and should be sized by MSP basis the Guiding principles of the IT infrastructure design section (On-Demand vs Fixed Billing). However, from a GeM perspective, the billing would be done quarterly irrespective of the Fixed/On-Demand model with the Cloud Service Provider.
6	The MSP should use Open-Source Solution (Enterprise Edition) for any application software that MSP would be deploying on Virtual Private Cloud/ Government Community Cloud. In case there is a need to purchase COTS (Commercial-off-the-Shelf) license, the same should be flagged and justified; additionally, any purchase of any license or support should be in the name of GeM.
7	The MSP should specify DC and DR locations. GeM may, at any point in time, ask to check for updated and valid STQC certification as part of the MSP being MeitY empaneled

#	Details
8	MSP should provide direct leased-line connections between DC/DR and GeM sites. Further, MSP is to size the bandwidth requirements for the same.
9	GeM Solution and Cloud services should be accessible via the internet and MPLS.
10	DC & DR should be compliant with SOC audits and should be provided by the same CSP.
11	The solution should have the ability to automatically provision services via a Web Portal (Self Provisioning), provide metering and billing to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota, and show-back information is essential for the virtual private cloud/GCC platform to be offered.
12	MSP, in alliance with the CSP, should ensure seamless migration in case the underlying processor architecture is upgraded.
13	The Virtual Private Cloud Services/Government Community Cloud Services of MSP should provide data migration services (both egress and ingress).
14	It is expected that the MSP will provide an integrated solution, after due consideration to the compatibility issues between various components. If there is a problem with compatibility between components, the MSP should replace the components with an equivalent or better component (that is acceptable to GeM) at no additional cost to GeM and without any project delays.
15	The Virtual Private Cloud/GCC Services of MSP should provide REST-based API for each of the services for automation along with SDKs for platforms like Microsoft .net, Java/JavaScript, Python, PHP or Ruby. The MSP should be able to utilize these API's to set up routine jobs such as backup on an automated schedule wherever necessary.
16	The Virtual Private Cloud/GCC Services of MSP should also provide API Gateway services to create, host, monitor API services that may be required as part of the solution.

Table 97: CSP general requirements

8.3.2 Policy Requirements

#	Details
1	The MSP should confirm that data will reside in India and should not be accessed by any entity outside the control of GeM.

#	Details
2	The "GeM Data" and "Virtual Private Cloud Services/Government Community Cloud Services of CSP Infrastructure" must be maintained ONLY at the declared hosting site of MSP which should be communicated as part of the solution document.
3	The MSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of the Government Department.

Table 98: CSP policy requirements

8.3.3 Logical Partitions

#	Details
1	All the applications would follow a three-tier architecture with a clear separation of database tier/layer from application and web layers. For microservices-based architecture, MSP should deploy Presentation, Logic and Database category of microservices on different VMs/Containers/ Alternates in IaaS.
2	The Web layer for applications accessed via Internet/MPLS WAN shall be hosted in the DMZ zone/Subnet; the application layer should be hosted in the Militarized Zone or a separate subnet.
3	The Database nodes (RDBMS) should be in a separate zone with higher security.
4	All management servers which are not directly accessible through the internet will be kept in Management Zone. Active directory, Different modules of Enterprise Management Servers (including network, server, database, helpdesk etc.), Single-Sign-On, access and identity management server, Security Operations Centre, etc., will be a part of this management layer.
5	There will be separate VLANs/Subnets created for Development, Training, UAT and Production environment to segregate development and testing traffic from the production. Appropriate firewall policies can be implemented to have further security between different zones.
6	For the purpose of sizing, the MSP would size the solution on Development, User Acceptance Testing (UAT), Training, and Production Environment. Please refer to the "High Availability" Guiding principle for sizing guidelines. Those guidelines should be used for sizing and pricing the solution. However, the solution should be scalable and sized on the cloud knowing that these guidelines can change in the future depending upon the requirement.

8.3.4 Configuration

#	Details
1	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput and hence once provisioned it should be possible to configure the IOs
2	The MSP should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.
3	The MSP shall ensure that identity solutions are utilized and use best practices like least privilege, changing of passwords regularly, enabling Multi-Factor Authentication for Privileged user or for Secure Delete are utilized.
4	Cloud service should support parameterization for a specific configuration.

Table 100: CSP configuration requirements

8.3.5 Services

#	Details
1	The MSP should own and offer services like Database as a service, DNS, Data warehouse Analytics, Message queuing; such services are preferred to be managed from a single console.
2	The MSP should offer support at any time, 24 hours a day, 7 days a week, and 365 days per year via phone, chat, and email.
3	The MSP should provide a web interface with support for multi-factor authentication to access and manage the resources deployed in the cloud.
4	Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines.
5	Provide Audit logs of the account activity to enable security analysis, resource change tracking, and compliance auditing.

#	Details
6	Provide data migration services either with the help of a Cloud Native or SaaS/Third-Party Software Deployed on VMs/ Containers/ Alternates solution for moving data of all types and sizes into and out of the cloud.

<div align="center">**Table 101: CSP services requirements**</div>

8.3.6   Compute

#	Details
1	The system must be Scalable, Reliable, Highly Available & should provision to upgrade/downgrade virtual machines/ containers/ alternates configuration parameters seamlessly based on demand.
2	The IaaS service should have the ability to Auto-Scale (Horizontal) on demand. The service should support automatically launching or terminating instances based on parameters such as CPU utilization or other factors basis the demand. The solution should also be able to do continuous monitoring and optimization of auto-scaling rules and limits. The Cloud service should have self-service provisioning where there are zero dependencies on CSP, and MSP should be able to provide the service in an agile manner without any intervention from CSP.
3	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
4	The MSP shall ensure that the database layer for the applications in production shall be deployed in N+N High availability mode. The Web and Application layer for the applications in production shall be deployed in N+1 high availability mode (Active-Active). However, the choice of Active-Active at the Application layer is upon the MSP.
5	The MSP shall ensure that the services that are deployed on partitions/virtual images and are required in the cluster and/or load-balancing mode, shall be deployed in such a manner that the load sharing/failover is across the OS instances and NOT amongst partitions of the same OS instance. In case of a hardware or software component failure in one partition, other partitions must not be shut down or rebooted.
6	Please remark on the core: vCPU ratio that would be used while giving out the VMs (if applicable).
7	Please confirm that for production instances no burstable vCPU/shared vCPU would be used.

<div align="center">**Table 102: CSP Compute requirements**</div>

8.3.7 Networking

#	Details
1	Cloud service should entail the use of Virtual Private cloud or GCC which would ensure logical isolation of the infrastructure.
2	Cloud service should be able to support multiple (primary and additional) network interfaces. Cloud service should be able to support multiple IP addresses per instance.
3	MSP should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
4	The MSP should provide mechanisms to establish private connectivity (IPSec) between the cloud environment and a stakeholder data centre, office, or colocation environment. The MSP should provide site-site VPN over direct peering/carrier peering to NIC POPs, site-site VPN for MSP data centre for operations management
5	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
6	The MSP must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
7	Cloud service should support a Hardware/Software-based VPN connection from the cloud DC/DR to GeM office & MSP premises.
8	Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.
9	Cloud service should support Load balancing (both local and Global) of instances across multiple host servers.
10	Cloud service should support multiple routing mechanisms including round-robin, failover, sticky session etc.
11	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
12	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.

#	Details
13	The MSP should be able to provide a minimum 10 Gbps network connectivity between the servers. MSP should periodically review network connectivity requirements and upgrade as needed.
14	The internet bandwidth shall be clean with DDOS protection and active monitoring to be provided by the ISP or by the MSP.
15	The Virtual Private Cloud /Government Community Cloud Services should have the following service available 1. IPv4, IPv6 2. DHCP (if needed) 3. IPSec VPN Tunnel Creation 4. SSL VPN 5. DNS services 6. Geo Load Balancer (Balancing between multiple sites) 7. L4 and L7 Load Balancer 8. At least L3,4,6,7 Anti-DDoS solution

Table 103: CSP networking requirements

8.3.8 Storage

#	Details
	Block
1	The MSP should offer block storage volumes greater than 1 TB in size.
2	Cloud compute service should support local storage for transient block storage requirements.
3	Cloud service should support solid-state drive (SSD) backed storage media that offer single-digit millisecond latencies. There should be an option to choose the media type with respect to the type of environment. All production instances storage should be SSD backed. Other environments need not be on SSD.
4	Data at Rest and Data in transit should be encrypted with customer-owned keys. Cyphers should be at least 256-bit Advanced Encryption Standard (AES-256).
	Object
1	The MSP should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data on demand.

#	Details
2	The MSP should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.
3	Data at Rest and Data in transit should be encrypted with customer-owned keys. Cyphers should be at least 256-bit Advanced Encryption Standard (AES-256).
4	Cloud Service should support lifecycle management configuration.
5	The place where the objects would be stored should be configurable and all objects should stay in India.
6	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).
7	Cloud service should be able to provide audit logs on object storage buckets/containers which should include details about access requests and error codes.
File Storage	
1	The MSP should offer a simple scalable file storage service to use with compute instances in the cloud.
2	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS/SMB connections.
3	Cloud service should support scalable IOPS and throughput performance at the required scale.
4	Data at Rest and Data in transit should be encrypted with customer-owned keys. Cyphers should be at least 256-bit Advanced Encryption Standard (AES-256).

Table 104: CSP storage requirements

8.3.9 Backup

#	Details
1	The MSP should offer a service with the ability to take regular and scheduled backup.
2	The MSP should propose a cloud-native solution or use a SaaS-based/Third-Party Software deployed on VMs/ Containers/ Alternates based backup software.

#	Details
3	Low-cost Object Storage should be utilized as the backup target. If there is a need to use the block-based storage for a backup target for staging or as a whole, the same should be flagged and explained.
4	The MSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications. Backup restoration should give confidence that the whole or critical impact areas can be restored successfully. Below are indicative guidelines and final decision on retention period should be taken in mutual agreement with GeM during requirements gathering: 1. An Initial Full Backup 2. Daily Incremental with 15 days retention 3. Weekly full with 30 days retention 4. Monthly Full with 30 days retention on Object Storage and 12 months retention on Long Term storage 5. Yearly Full with 30 days retention on Object storage and 7 Years retention on Long term storage 6. For the databases, perform a twice-weekly full database backup, with three times daily backup of database log files 7. Encryption of all backup files and data and management of encryption keys as a service that can be enabled for GeM that require such a service 8. Backup restoration practices should comply to the data integrity standards 9. Different Tiers of Backup storage should be chosen depending upon the reads/restore that would be required 10. Restoration Policies: a. Backups are taken in the last 2 months: Once in a month b. Backups are taken in the last 6 months: Once in a Quarter c. Backups are taken in last 1 Year: Once in Half Year d. The restoration would be performed on a random basis and would be done against a ticket logged in the ITSM tool. <table><tr><td>#</td><td>Backup Type</td><td>Backup Frequency</td><td colspan="2">Retention Period</td></tr><tr><td></td><td></td><td></td><td>Object Storage</td><td>Long term Storage</td></tr><tr><td>1</td><td>Daily Backup</td><td>Daily Incremental</td><td>15 days</td><td>Not Required</td></tr></table>

#	Details				
	2	Weekly Backups	Weekly Full	30 days	Not Required
	3	Monthly Backup	Monthly Full	30 days	12 months
	4	Yearly Backup	Yearly Full	30 days	7 years
5	Any data requested from Long Term Storage should be retrievable within a time span of 12 hours.				
6	The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policies for a section of data that requires the same.				
7	Data at Rest and Data in transit should be encrypted with customer-owned keys. Cyphers should be at least 256-bit Advanced Encryption Standard (AES-256).				
8	Data archiving is the practice of shifting infrequently accessed data to low-cost storage repositories. It is an important part of a data management strategy. The goal is to reduce costs on warm storage while retaining old data needed for future reference or analysis, and information needed for regulatory compliance.				

Table 105: CSP backup requirements

8.3.10 Disaster Recovery

#	Details
1	The solution should be architected to run on cloud services offered from multiple data centre facilities to provide business continuity with no interruptions in case of any disruptions /disaster to one of the data centre facilities. In case of failure, automated processes should move customer data traffic away from the affected area. The Cloud Service Provider should provide adequate bandwidth between the Data Centre Facilities to provide business continuity.
2	DR should be available at the time of the disaster at DC. MSP should size the solution as per defined RPO and RTO in SLAs provided in Volume 1 Section 8.6 of this RFP.
3	In the event of a Primary site failover or switchover, the DR site should take over the active role, and all requests should be routed through that site.
4	MSP should offer switchover and switchback of individual applications (from a services standpoint) apart from the entire system.

#	Details
5	In case of failover to the DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for the RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.
6	In case of disaster at the DC site (within the defined RTOs and RPOs), the DR should be available (with its data) on-demand basis, wherein 100% of the services of DC would run from the DR site (after the RTO time and with the RPO level). Once the DC is restored, failback to DC is to happen.
7	DC and DR should follow like to like Architecture and capacity and in terms of all the environments required to be provisioned for the GeM project.
8	CSP shall follow the following key guidelines w.r.t the DC-DR Drill: 1. CSP needs to allocate adequate resources, do project management and work closely with the MSP for performing the DC-DR Drills whenever planned by the Purchaser. 2. Any configuration level changes which can impact the DC-DR drill need to be informed by the MSP to CSP team before handover to avoid issues during the drill. 3. During DC-DR drill CSP needs to allocate appropriate resources onsite to avoid any failure and delays. 4. CSP needs to perform project management and all reporting and pre- and post-environment preparation to avoid any failure in the drill. 5. CSP needs to ensure successful replication between production. 6. CSP needs to perform periodic recovery testing. 7. CSP needs to develop and execute test plans as per defined periodicity or as and when required. 8. CSP needs to coordinate with all the users involved in DR testing. 9. CSP needs to track and report DR test results. 10. CSP needs to develop an action plan and timeline to address DR testing results. 11. CSP needs to implement DR action plans and provide ongoing status reporting until completion of all action items. 12. GeM can also do an unplanned DC-DR drill which CSP needs to support and design the system accordingly.

Table 106: CSP disaster recovery requirements

8.3.11 Security Guidelines

#	Details
1	The Virtual Private Cloud/GCC Services shall be fully secure with no scope of data breach/leaks/thefts/data mining/privacy breach etc. It would be MSP responsibility that for the layers where MSP is managing (For example in IaaS, above Hypervisor) all the relevant security layers are deployed. MSP should also ensure that CSP is also fulfilling all its responsibility (For example, in IaaS, Hypervisor and below, Physical, Network, Perimeter etc.).
2	The security services/tools should be dedicated (virtual/physical) to the GeM solution.
3	The MSP shall be responsible for ensuring the security of GeM applications and infrastructure from any threats and vulnerabilities. The MSP shall address ongoing needs of security management including, but not limited to, monitoring of various devices/tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules.
4	The MSP should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.
5	Cloud service should offer a secure way to login (like public and private keys) and should have audit details which should tell about the keys last use details support reporting a user's access keys last use details.
6	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.
7	Cloud service should support a policy validator to automatically examine non-compliant access control policies.
8	Cloud service should support features such as user and group management.
9	Cloud service should allow users to reset their passwords in a self-service manner.
10	The MSP should offer HSM modules.
11	The MSP should offer a service to create and control the encryption keys used to encrypt user data.
12	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry-standard AES-256 or equivalent cryptographic algorithm. Data at Rest and Data in

#	Details
	transit should be encrypted with customer-owned keys. Cyphers should be at least 256-bit Advanced Encryption Standard (AES-256).
13	Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
14	Cloud Service should also provide for Database Activity Monitoring (DAM) and alternate processes for continuity in monitoring of processes in case of failure of DAM.
15	The MSP shall be responsible for ensuring the security of GeM applications and infrastructure from any threats and vulnerabilities. The MSP shall provision and monitor the following security layers 1. Layer 4 Firewall 2. Layer 7 Firewall (WAF) 3. Intrusion prevention/ detection (Network and Host level) 4. Content filtering and blocking 5. Virus protection 6. Event logging & correlation 7. Vulnerability protection through implementation of proper patches and rules. 8. Vulnerability Assessment and Penetration testing before Go-live of any module 9. Database Activity Monitoring 10. Hardware Security Module 11. Multi Factor Authentication 12. Web Gateway with Content Filtering and Proxy Solution 13. Anti-Advanced Persistent Threat 14. Anti-DDoS 15. Anti-Virus 16. Data Leakage Prevention 17. SSL VPN 18. Email Gateway 19. Privileged Identity Management

Table 107: CSP security requirements

8.3.12 Data Security & Information Lifecycle Management

#	Details

#	
1	Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
2	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.
3	Multi-tenant organizationally owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: 1. Established policies and procedures 2. Isolation of business-critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance 3. Compliance with legal, statutory, and regulatory compliance obligations

Table 108: Data security & information lifecycle requirements

8.3.13 Identity & Access Management

#	Details
1	The Virtual Private Cloud/Government Community Cloud Services should provide Identity and Access Management service for the layer managed by MSP. MSP should bring in identity and access management solution (3rd Party or Cloud-Native) for the layer that would be managed by them (For example, OS and above in case of IaaS). The solution should ensure that features like Multi-factor Authentication(Physical token-based or Virtual Token Based), enforceable password policies, defining of roles both for resources and users, federation capabilities with other 3rd party Directory Services are present.
2	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally owned or managed (physical and virtual) application interfaces and infrastructure network and systems components.
3	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

8.3.14 Incident Response

#	Details
1	The MSP should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure networks and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The MSP must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures.
2	The Solution shall comply with ITIL (Information technology Infrastructure Library) standards.
3	The MSP must bring in an ITSM tool through which the tickets can be logged in.
4	The MSP should have proper forensic procedures defined and implemented, including chain of custody, required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.
5	A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs the customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part of the service and/or the customer (tenant) has some shared responsibility for implementation of control.

Table 110: Incident response requirements

8.3.15 Governance & Risk Assessment

#	Details
1	The MSP should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design,

#	Details
	implementation, testing, use, and monitoring of deployed or engaged services in the cloud.
2	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.
3	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective
4	The solution shall have audit and compliance features that enable the Client agency to monitor the provisioned resources, performance, resource utilization, and security compliance. It shall have the following functionalities:
5	The solution should have an automated security assessment service that should provide the following: a. vulnerabilities assessment services b. Penetration Testing services c. deviations from best practices such as password policy, unnecessary opened firewall ports, storage access policy, the suggestion of data to archive
6	The system should have the ability to set up alarms basis resource usage and the ability to define actions on triggering of those alarms(For example, the ability to send an email when storage utilization has crossed x% or archive a storage section depending upon data type when it has crossed x% utilization)
7	Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
8	The solution should provide a dashboard that would list the details of any planned maintenance scheduled as well as any unplanned downtime faced in the recent past(past 3 months at least).
9	MSP should provide a dashboard for monitoring the RPO and RTO of each application and database. The Dashboard should clearly show the data replication process and any lag/failure in data replication that should be notified through alerts to respective authorities.
10	The solution should be able to log all account and resource access into the account and resources (which might be resources logging into the account using API call or root/admin users or other users logging into the account).
11	The solution should be able to discover all provisioned resources in the Virtual Private Cloud Services/Government Community Cloud and provide details such as configuration items inventory, history of changes to such configuration items, a snapshot of resource inventory at a single point in past, set-up of policies to track the provision of resources

#	Details
	within client-defined rulesets and auto-notifications each time a configuration change occurs.
12	The solution should be able to suggest best practices to optimize the overall cost of resources.

Table 111: Governance & risk requirements

8.3.16 Compliance

#	Details
1	The MSP should understand and incorporate the different types of laws and regulations that impose security and privacy obligations on the organization. Especially those pertaining to data location, privacy and security controls, records management, and electronic discovery requirements.
2	The MSP should ensure that independent reviews and assessments are conducted at least annually to ensure that the organization addresses nonconformities with the established policies, standards, procedures, and compliance obligations.
3	New GeM platform should comply with international security standards such as ISO27001, ISO 27017, ISO 27018, etc.

Table 112: Compliance requirements

8.3.17 Business Continuity Planning

#	Details
1	MSP shall define and submit (as part of the solution), a detailed approach for "Business Continuity Planning"; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which "disaster" would be declared.
2	The MSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.

#	Details
3	The MSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.
4	Incident response plans should be developed by the MSP which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

Table 113: Business continuity planning requirements

8.3.18 Monitoring Solution

#	Details
1	GeM intends to monitor operational activities to have a holistic view of the provisioned cloud services and their configurations to ascertain required features have been appropriately implemented. In this view, the MSP shall provision and implement monitoring tools (third party or cloud-native) for measuring the service levels and application/ server/ storage/ network performance & utilization. Basis the inputs of the Monitoring Solution, the cloud services should be configurable with auto-change in provisioned resources as per the monitoring inputs.
2	The monitoring tool should publish (on the portal) real-time status (of all the services) that is refreshed with at least 5 min frequency; further, the tool should publish all historical parameters for a period of a minimum of 3 months. The tool shall be capable of generating per day/month/quarter utilization reports
3	The monitoring system should have the following components:
3.1	Cloud Dashboards: Collect and track metrics, collect and monitor log files, and set alarms to gain system-wide visibility into resource utilisation, application performance, and operational health. Overall, the monitoring platform should provide End to End monitoring of complete IT Infrastructure
3.1.1	Server Monitoring: Should monitor heterogeneous operating systems for both dedicated & virtual instances on MSP OS layer including (but not limited to) Windows 32/64 bit, all major flavours of Linux, etc.
3.1.2	Application Monitoring: To perform infrastructure aware application triage, i.e., pinpoint network issues causing application degradation. The MSP should also deploy polling tools at the end-user site/GeM offices to measure performance SLAs(with Synthetic User Monitoring and Real User Monitoring)

#	Details
3.1.3	Database Monitoring: Monitor multiple database servers and versions being proposed on each server
3.1.4	Storage Monitoring: Monitor IOPS, Latency etc.
3.1.5	Network Monitoring: Should provide the capability to monitor any device based on SNMP v1, v2c & 3
3.1.6	SLA Monitoring: Support Service Level Agreements, Lifecycle Management including Version Control, Status Control and Audit Trail
3.2	Audit Trail: Provide logs of all user activity. The recorded information should include (but not be limited to) the identity/source IP of the API caller, time of API call, the request parameters, and the response elements.
3.3	Security Compliance: Monitors cloud resources and provide alerts in regard to security gaps such as overly

Table 114: Monitoring requirements

8.4 Annexure D - Sizing Considerations

Below given are indicative sizing requirements for the new GeM platform. However, this is to be noted that these are only directional requirements, and the MSP will need to provide exact sizing estimates basis on the understanding of the requirements and provision for at least 5 times of the sizing estimates as buffer capacity. In addition, sizing should be reviewed at the start of each Financial year throughout the duration of this contract and necessary additions should be done in alignment with competent authority at GeM so that the sizing is always sufficient to cater to the required Service Levels mentioned in Volume 1 Section 8.6 of this RFP.

#	Parameter	Description	Sizing Estimations
1.	Network Connectivity	Network Connectivity within Cloud Services	Minimum 10 Gbps betweenServers
2.	Blade Server, RackServer	Compute Capacity in CloudServices	Minimum 10 GB ports
3.	CPU	Utilization upper limits	70%
4.	Cloud Compliance Standards	ISO 27001	ISO 27017, ISO 27018
		Security	SOC 1 & SOC 2
5.	Storage	Physical read	As suitable

		Physical write	As suitable
		Volumes	Disc > 1 TB
		Media	SSD
6.	Database IOPS	Main Transaction TableSpace	As suitable
7.	Re-size/ headroom	Virtual Cores, Memory, andStorage Seamlessly	As suitable
11.	Concurrent Users	Concurrency at Peak Load	20-25% of transacting users on GeM
13.	Storage	Static & Transaction data	Directionally 15-20 GB per contract transaction on GeM
14.	Aadhar authentication	Buyers and Sellers	No. of authentications reqd. per contract / transaction is 8-10
15.	SMS gateway	Buyers and Sellers	No. of SMS notifications / OTPs reqd. per contract / transaction is 6-8

8.5 Annexure E - Manpower Requirements

8.5.1 Manpower requirements

1. The MSP shall provision for required resources for development and implementation of new GeM platform, Operations & maintenance of the current GeM platform till new platform Go-live, and Operations & maintenance of the new GeM platform after Go-live throughout the duration of this contract. Accordingly, MSP shall deploy the minimum number of resources in 3 separate teams as defined below:

    a. **Team A:** New Platform development and implementation till Go-live, organized into agile squads and core team, as needed

    b. **Team B:** Knowledge transfer on the current platform and resources ramp-up till the new platform Go-live (in line with Volume 1 Section 5 of this RFP)

    c. **Team C:** Operations and maintenance of the GeM platform (either current or new as applicable) after the date of expiry of outgoing MSP contract i.e., 1st January 2024

2. MSP should ensure that there should be no personnel overlap across above defined teams, other than explicitly specified by GeM in this RFP. After the Go-live of new GeM platform, 30%

personnel of Team A and 30% personnel of Team B shall mandatorily be a part of Team C till at least 12 months post Go-Live.

3. For avoidance of doubt, nothing in this RFP requires, or should be construed as requiring, MSP to provide legal, tax or accounting advice or opinion to GeM. Any information provided in connection with the Services will not be construed as legal advice and will not be intended to be a substitute for legal counsel on any subject matter. GeM acknowledges and agrees that MSP does not provide GeM with legal advice of any kind in connection with the Services.

4. Contact Center & Technical Helpdesk resources as mentioned in below tables (i.e., Account Head, Manager (Training & Quality) and Manager (Data Analytics-cum-MIS)) must be MSP resources and shall be on MSP payroll. In addition to these resources, MSP/ sub-contractor shall deploy additional resources for each contact center facility in accordance with minimum resource requirements stipulated in Volume 1 Section 3.1.7.2 and the support ratios defined in Volume 1 Section 3.1.7.4 of this RfP.

8.5.1.1   Team A: Key Resource Requirements (Minimum – Indicative)

#	Named Resources	Category	Minimum quantity
1.	**Project Director** **(common across Team A, B and C)**	**C1**	**1**
Business Service Unit (BSU)			**1**
2.	Procurement Domain Expert	C1	1
Technical Service Unit (TSU) – Platform development			**181**
3.	Technical Program Manager	C1	3
4.	Enterprise Architect	C1	1
5.	Solution Architect	C1	2
6.	Senior Technical project manager	C1	3
7.	Project manager – Technical services	C1	9
8.	Product manager	C2	9
9.	Scrum Master	C2	9
10.	Senior DevOps engineer	C2	12
11.	DevOps engineer	C3	16
12.	Microservices Architect	C3	27
13.	Full stack developer	C3	27

#	Named Resources	Category	Quantity
14.	Security Expert	C3	10
15.	CI-CD based Unit & Integration tester	C3	35
16.	Pilot deployment specialist	C2	1
17.	UI/UX Lead	C2	3
18.	Business analyst	C2	8
19.	Data migration and cutover expert	C2	4
20.	AI/ML Expert	C3	2
Total resources			**183**

8.5.1.2   Team B: Key Resource Requirements (Minimum – Indicative)

#	Named Resources	Category	Minimum quantity
1.	**Project Director** **(common across Team A, B and C)**	**C1**	**1**
Business Service Unit (BSU)			**24**
2.	Manager - Buyer & Seller Management	C2	1
3.	Consultant - Buyer & Seller Management	C3	15
4.	Manager - Buyer and Seller Training	C2	1
5.	Consultant - Buyer and Seller Training	C3	4
6.	Account Head - Contact Centre & Technical Helpdesk	A1	1
7.	Manager (Training & Quality) - Contact Centre & Technical Helpdesk	A2	1
8.	Manager (Data Analytics-cum-MIS) - Contact Centre & Technical Helpdesk	A2	1
Technical Service Unit (TSU)			**51**
9.	Senior Technical project manager	C1	2
10.	UI/UX Lead	C2	1
11.	Business analyst	C2	2
12.	Full stack developer	C3	6
13.	Product manager	C2	6
14.	CI-CD based Unit & Integration tester	C3	6

#		Category	Minimum quantity
15.	Senior DevOps engineer	C2	10
16.	DevOps engineer	C3	11
17.	Security Expert	C3	7
Total resources			**76**

8.5.1.3   Team C: Key Resource Requirements (Minimum – Indicative)

#	Named Resources	Category	Minimum quantity
1.	**Project Director (common across Team A, B and C)**	**C1**	**1**
Business Service Unit (BSU)			**73**
2.	Manager - Buyer & Seller Management	C2	3
3.	Consultant - Buyer & Seller Management	C3	45 (across states)
4.	Manager – Buyer and Seller Training	C2	2
5.	Consultant – Buyer and Seller Training	C3	15
6.	Account Head – Contact Centre & Technical Helpdesk	A1	1
7.	Manager (Training & Quality) – Contact Centre & Technical Helpdesk	A2	1
8.	Manager (Data Analytics-cum-MIS) – Contact Centre & Technical Helpdesk	A2	1
9.	Procurement Domain Expert	C1	2
10.	Manager - Marketing & Promotions	C2	1
11.	Executive - Marketing & Promotions	C3	2
Technical Service Unit			**146**
12.	Technical Program Manager	C1	3
13.	Chief Enterprise Architect	C1	1
14.	Enterprise Architect	C1	1
15.	Solution Architect	C1	3
16.	Project manager – Technical services	C1	3
17.	Project manager – Payment	C1	1

18.	Senior technical project manager	C1	1
19.	Product manager	C2	3
20.	Scrum Master	C2	9
21.	Senior DevOps engineer	C2	14
22.	DevOps engineer	C3	23
23.	Integration engineer	C3	5
24.	Microservices Architect	C3	9
25.	Senior full stack developer	C2	7
26.	Full stack developer	C3	12
27.	Developer – Payment	C3	2
28.	Security Expert	C3	11
29.	CI-CD based Unit & Integration tester	C3	17
30.	UI/UX Lead	C2	2
31.	Business analyst	C2	8
32.	BI analysts cum data pipeline modeler	C3	5
33.	AI/ML Expert	C3	4
34.	Project Manager – Cloud / Representative from CSP	C2	2
Contract management unit			**2**
35.	Head – Legal matters	C2	1
36.	Manager – Contract Administration	C2	1
Total resources			**222**

8.5.2 Manpower profiles

Below given are indicative qualification and experience requirements for the profiles to be deployed by the MSP. This is to be noted that these are only directional requirements, and the MSP should deploy best of class professionals to ensure successful execution of this project throughout the contract duration. All the profiles to be deployed by the MSP should have:

1. Excellent oral and written skills to be able to facilitate discussions and reach decisions

2. Good analytical and problem-solving skills

8.5.2.1 Project Director – GeM

8.5.2.1.1 Qualifications

1. Must possess graduate degree in Technology / Engineering and/ or Post-graduate degree in Management

2. Certification in Program/Project Management is preferred

8.5.2.1.2 Experience

1. Must have at least 15 years of relevant experience

2. Should have successfully delivered at least two large managed SI projects involving Software Application design, development & maintenance, cloud operations & maintenance, OR related to e-procurement or e-commerce portal

3. Must have managed in the capacity of Project Director/Program Manager for a project with TCV more than INR 600 Crore

4. Experience in project management in Government sector is preferred

8.5.2.1.3 Roles and Responsibilities

1. Responsible for organizing, planning, directing and coordinating overall program effort

2. Should have extensive experience and proven expertise in managing similar contracts

3. Establish overall GeM project management strategy

4. Link objectives of the GeM program and the technical solution being implemented

5. Implement GeM Implementation Strategy and Plan

6. Participate in direct development of commissioning strategy

7. Monitor overall project progress and provide direction

8. Responsible for periodically assessing the project resourcing and ensuring it is in line with proposed deployment and adequate for project requirements

9. Assess project risks and ensure timely resolution

10. Ensure compliance to the terms and conditions of contract and SLAs

11. Convene Steering Committee meetings as scheduled to ensure timely action

8.5.2.2 Manager – Buyer & Seller Management

8.5.2.2.1 Qualifications

1. Must possess post-graduate degree in Management or Technology
2. Certificate in Project Management, Program Management are desirable

8.5.2.2.2 Experience

Total work experience of at least 8 years and at least 4 years of experience in e-commerce industry/ Business development/ Technical support

8.5.2.2.3 Roles and Responsibilities

1. Own and drive successful execution and delivery of Buyer and Seller Management services
2. Act as an onsite Point of Contact for different Buyer departments or states
3. Effectively manage support for multiple Buyer and Seller stakeholders – registration, business processes, payment & delivery, and marketing & promotion
4. Handling end to end issues, disputes and any grievance related to the client and escalating them to the relevant authorities at GeM
5. Act as a liaison between GeM and the parties (both Buyers and Sellers)
6. Setting up internal review meetings to check the progress of Buyer and Seller management done by the associates
7. Influence business services leadership to create and maintain alignment around the GeM platform deliverables, success criteria, scope, and constraints
8. Coordinate efforts of all agencies associated with the MSP (sub-contractors, consortium partners) in the delivery of these services
9. Identify areas of process improvement and innovation & lead implementation of the same
10. Responsible for the implementation of continuous improvements in the Buyer and Seller management team in the Business Services Unit and achievement of Key Performance Indicators and deliverables specified by GeM

8.5.2.3 Manager – Buyer & Seller Training

8.5.2.3.1 Qualifications

1. Must possess post-graduate degree in Management or Technology
2. Certificate in Project Management, Program Management are desirable

8.5.2.3.2 Experience

Total work experience of at least 8 years and at least 4 years of experience in e-commerce industry with prior experience in conducting business trainings

8.5.2.3.3 Roles and Responsibilities

1. Follow GeM's training plan and assign trainers in online/ offline mode trainings for Buyers and Sellers
2. Identify need for training across different Buyers and Seller based on product or service categories or ratings on the GeM platform
3. Evaluate GeM training programs basis metrics like engagement level, training feedback etc and design new programs
4. Collate feedback from Buyers and Sellers on training and other performance enhancement programs.
5. Analyze course evaluations to determine effectiveness of training sessions and to recommend/implement improvements
6. Serve as a key subject matter expert and mentor to Buyer and Seller management consultants
7. Ensure proper following of GeM's training plan and provide feedback to trainers to improve performance based on identified performance metrics.

8.5.2.4 Consultant – Buyer & Seller Management

8.5.2.4.1 Qualifications

Regular full-time B.Tech./B.E/MCA OR regular full-time Post-Graduate Degree/ Diploma in Management

8.5.2.4.2 Experience

Total work experience of 2 years in e-commerce industry or public procurement or business development

8.5.2.4.3 Roles and Responsibilities

1. Own and drive successful execution and delivery of Buyer & Seller Management services
2. Act as an onsite Point of Contact for different Buyer departments or states
3. Effectively manage support for multiple Buyer and Seller stakeholders – registration, business processes, payment & delivery, and marketing & promotion
4. Handle end to end issues, disputes and any grievance related to the client and escalating them to the relevant authorities at GeM
5. Act as a liaison between GeM and the parties (both Buyers and Sellers)

8.5.2.5 Consultant – Buyer & Seller Training

8.5.2.5.1 Qualifications

Regular full-time B.Tech./B.E/MCA OR regular full-time Post-Graduate Degree/ Diploma in Management AND/OR some relevant work in training area for an e-commerce platform

8.5.2.5.2 Experience

Total work experience of at least 2 years in e-commerce or public procurement with prior experience in conducting business trainings

8.5.2.5.3 Roles and Responsibilities

1. Identify business needs and design general training programs for GeM portal users
2. Follow GeM's training plan and ensure satisfactory score in all trainer assessments.
3. Collate Buyer and Seller feedback on training and other performance enhancement programs.
4. Analyze course evaluations by tracking engagement rates to determine effectiveness of training sessions and to recommend/implement improvements
5. Achieve the budgeted trainer man-days of delivery across the allocated skill set (as per the learning roadmaps).

8.5.2.6 Account Head - Contact Centre & Technical Helpdesk

8.5.2.6.1 Qualifications

1. Must possess post-graduate degree in Management or Sales, Marketing, or related fields
2. Certificate in Project Management, Program Management are desirable
3. Deep knowledge in continuous improvement methods such as Kaizen, Lean, DMAIC, etc. is required

8.5.2.6.2 Experience

Minimum 13 years of professional experience in Customer Service or Technical helpdesk with experience in e-commerce industry preferred

8.5.2.6.3 Roles and Responsibilities

1. Developing and managing contact centre engagement with GeM
2. Achieving monthly performance targets by tracking and improving Contact Center SLAs
3. Responsible for developing, tracking, achieving and exceeding weekly and monthly KPIs
4. Closely work with GeM and MSP leadership to drive continuous improvement and manage business requirements, resource allocation plan, customer satisfaction, quality of resolution
5. Act as the thought leader and strategist for ideal user experience on GeM portal
6. Maintain and improve GeM contact centre operations by monitoring system performance; identifying and resolving problems; preparing and completing action plans; completing system audits and analyses

8.5.2.7 Manager (Training & Quality) – Contact Centre & Technical Helpdesk

8.5.2.7.1 Qualifications

1. Bachelor's or advanced degree in any field
2. Six Sigma knowledge / certification is preferred

8.5.2.7.2   Experience

Minimum 8 years of professional experience in Customer Service or Technical helpdesk

8.5.2.7.3   Roles and Responsibilities

1. Responsible for the overall direction, coordination, and evaluation of the training team under contact centre in accordance with the GeM policies and procedures

2. Prepare contact centre training reports by collecting, analyzing, and summarizing data and trends and present the same to GeM team

3. Improve Contact Centre Efficiency by regularly auditing and analyzing Contact Centre data. Based on the findings identify training opportunities to enhance GeM user handling skills.

4. Ensure proper following of training plan and provide feedback to trainers to improve performance based on identified performance metrics

5. Analyze course evaluations to determine effectiveness of training sessions and to recommend/implement improvements

6. Responsible for the overall direction, coordination, and evaluation of the quality assessment team under contact centre in accordance with the GeM policies and procedures

7. Consult with delivery leads, operations managers and team leads regarding quality monitoring trends, reports and recommendations.

8. Create quality assessment and improvement plans, review the design and deploy solutions with an ability to quantify results and share qualitative insights and collaborate with operations teams to ensure a better quality of interaction.

8.5.2.8   Manager (Data Analytics-cum-MIS) – Contact Centre & Technical Helpdesk

8.5.2.8.1   Qualifications

Graduate/post graduate degree in any discipline (preferably engineering, commerce, business, or related fields)

8.5.2.8.2   Experience

1. Minimum 8 years of experience in business operations and intelligence tools like SQL/ MIS/Advance Excel/ PowerBI with minimum 5 years' experience at contact centre

2. Prior exposure to MS office, business intelligence (BI) tools like PowerBI, Tableau, etc.

8.5.2.8.3 Roles and Responsibilities

1. Responsible for leading, developing and managing GeM Contact Centre's data analytics, reporting and strategic planning activities
2. Responsible for managing the MIS and data analytics team at contact center facilities
3. Maintain contact center data, and create monthly, weekly, & daily analysis reports and dashboards by making in-depth analysis to generate action items and improvement plans for GeM Contact Center team

8.5.2.9 Procurement Domain Expert

8.5.2.9.1 Qualifications

1. Graduate/post graduate degree in any discipline (preferably engineering, commerce, business, or related fields) with preference for MBA
2. Strong knowledge of government policies related to public procurement and contract management

8.5.2.9.2 Experience

Minimum of 15 years experience in public procurement and/or contract management domain

8.5.2.9.3 Roles and Responsibilities

1. Closely work with GeM on Buyer and Seller requirements, marketplace policy formulation, and continuous improvement in business processes
2. Ensuring that the policy is relevant and updated basis changing procurement landscape
3. Monitor & analyze policy issues and developments & provide strategic advice to senior GeM stakeholders
4. Work closely with communications team to create & execute compelling communication strategies around policy priorities
5. Identifying and addressing pain points and driving the adoption of the policy by the different Buyers

8.5.2.10   Manager – Marketing & Promotions

8.5.2.10.1   Qualifications

Regular full-time B.Tech./B.E/MCA OR Regular Full Time Post-Graduate Degree/ Diploma in Marketing/Management

8.5.2.10.2   Experience

1. Minimum 8 years of total marketing and promotion work experience and at least 5 of experience in e-commerce industry

2. Experience in analyzing market trends, developing methods of field-test on marketing programs to determine customer acceptance, evaluate effectiveness of promotion efforts and keep informed on needs of the various market segments

3. Excellent analytical skills and decision making ability

8.5.2.10.3   Roles and Responsibilities

1. Plan and launch promotion campaigns for GeM and analyze market trends via effective use of market research data

2. Develop comprehensive e-commerce marketing campaigns including management of calendar, creative brief, asset creation, scheduling, QA, approval, segmentation building, and in-depth post deployment analysis for GeM portal

3. Planning and implementation of marketing and promotion activities for branding GeM and drive greater adoption for the assigned products

4. Identify additional GeM portal improvement opportunities in short and medium term

5. Liaise with other cross functional teams and vendors for timely implementation of brand strategy

6. Partner with BI on the prioritization of the highest reporting, and insight generation to drive acquisition and retention improvements

8.5.2.11   Executive – Marketing & Promotions

8.5.2.11.1   Qualifications

1. Regular full-time B.Tech./B.E/MCA
2. An MBA in marketing or an equivalent master's degree is preferred
3. Strong negotiation, analytical and implementation skills

8.5.2.11.2 Experience

1. Minimum 2 years of relevant experience of working in either marketing or analytics
2. Experience of working in an analytical, results-oriented environment with external customer interaction

8.5.2.11.3 Roles and Responsibilities

1. Support the marketing team on ground by managing execution of marketing initiatives and campaigns across digital and offline channels
2. Analyze the market to see performance and updating the organization with new feedback on customer trends for holistic decision making
3. Explore new opportunities / platforms / affiliations to increase visibility for GeM campaigns across all platforms
4. Synthesize, analyze and report marketing program metrics. Track and monitor performance of the marketing campaigns.
5. Identify trends and drive innovation to develop new offerings for GeM portal

8.5.2.12 Senior Technical Project Manager

8.5.2.12.1 Qualifications

1. Graduate in Engineering/Computer Science/Information Technology
2. Preferred:
    o Advanced certifications in Software development lifecycle
    o Certificate in IT Project Management and CMMI
    o Advanced certifications in Service Delivery – ITIL v3

8.5.2.12.2 Experience

1. Should have at least 12 years of demonstrated relevant experience in IT projects and services management

2. Should have led at least three end-to-end large software delivery or product development assignments from design till roll out with exposure to setting up of IT infrastructure in cloud (data centre, network, security, and storage systems)

3. Should have experience in database, storage, networking and security architectures in clouds set up

4. Should have experience in working on large-scale distributed and heterogeneous IT systems in cloud set up

5. Experience in implementation of open standards and open-source technologies shall be preferred

8.5.2.12.3   Roles and Responsibilities

1. Responsible for all IT systems forming part of the GeM Technology Solution which will include the GeM-APP, cloud, Portal solutions, Cloud Network, Cloud Storage Systems, IT Security systems, GeM compute and non-compute components

2. Responsible for new application development, testing and release and delivery within the stipulated SLAs and specified contract conditions

3. Update and upgrade of the GeM portal and its related patches to improve system performance

4. Responsible for continuous monitoring and improvement in GeM portal performance and delivery as signed off by the Steering Committee and MSP

5. Responsible for implementation of IT security policies and procedures within the GeM solution

6. Ensure that all key networks especially the DC/DR cloud Network and GeM Office Networks are maintained as per the service levels agreed upon

7. Manage the team of administrators (server, storage, network, security) and their adequate deployment

8.5.2.13   Project Manager – Technical services

8.5.2.13.1   Qualifications

1. Graduate degree in Engineering/Computer Science/Information Technology

2. Preferred

a. Advanced certifications in Software development lifecycle

b. Certificate in IT Project Management and CMMI

c. Advanced certifications in Service Delivery – ITIL v3

8.5.2.13.2 Experience

1. Should have at least 8 years of demonstrated relevant experience in IT projects and services management

2. Should have led at least three end-to-end large software delivery or product development assignments from design till roll out with exposure to setting up of IT infrastructure in cloud (data centre, network, security and storage systems

3. Should have experience in database, storage, networking, and security architectures in clouds set up

4. Should have experience in working on large-scale distributed and heterogeneous IT systems in cloud set up with microservices architecture, agile streams, and domain driven business services

5. Should have experience in implementation of open standards and open-source technologies shall be preferred

8.5.2.13.3 Roles and Responsibilities

1. Responsible for all IT systems, domain driven services, forming part of the GeM Technology Solution which will include the GeM-APP, cloud, Portal solutions, Cloud Network, Cloud Storage Systems, IT Security systems, GeM compute and non-compute components

2. Responsible for new application development, testing and release and delivery within the stipulated SLAs and specified contract conditions

3. Update and upgrade of the software and its related patches to improve performance of the IT systems as signed off by the Steering Committee and MSP

4. Responsible for implementation of IT security policies and procedures within the GeM solution

5. Ensure that all key networks especially the DC/DR cloud Network and GeM Office Networks

are maintained as per the service levels agreed upon

8.5.2.14   Project Manager - Cloud/ Representative from CSP

8.5.2.14.1   Qualifications

1. B.Tech/B.E. in Computer Science
2. Master of Science/MBA would be a bonus
3. Strong leadership, project management skills, time management, and problem-solving skill

8.5.2.14.2   Experience

1. Minimum 10 years of experience in IT Infrastructure Delivery Management with at least 6 years of experience in cloud service project management in e-commerce industry
2. Prior experience with Scrum methodology and Agile practices is required
3. Prior exposure to large migrations and infrastructure automation is desirable

8.5.2.14.3   Roles and Responsibilities

1. Define, develop, communicate and maintain the delivery methodology for the implementation of new GeM portal on cloud
2. Produce supporting materials, including documentation and template project plans for use by project managers and MSP
3. Guide CSP team to increase efficiency by identifying bottlenecks, eliminating redundancy and tailoring SDLC processes to fit their needs
4. Analyze existing GeM application and Cloud platform technical requirements to enable functional, technical, and application migration changes for the new GeM portal by coordinating with CSP team
5. Manage change requests for all GeM cloud migration activities, and tracks all events associated with those activities in order to maximize systems availability and avoid errors
6. Ensure that dependencies, assumptions, risks and issues are identified, recorded and managed throughout the SDLC and flagged to GeM team.

8.5.2.15 Technical Program Manager

8.5.2.15.1 Qualifications

1. Post-Graduate degrees in Management/Computer Science/Information Technology/ M.Tech.
2. Certificate in ITIL v3, Project Management, IT Technology Service Management are desirable

8.5.2.15.2 Experience

1. Must have at least 10 years of demonstrated relevant experience in IT services
2. Experience in managing large IT project implementations across all stages from design till steady state operations
3. Experience in management of at least one major transition project
4. Experience in end-to-end management of one e-commerce project
5. Experience in working on large-scale distributed and heterogeneous IT systems preferred

8.5.2.15.3 Roles and Responsibilities

1. Own and execute SDLC for one or more top level key technical initiatives by partnering with Project Sponsors, other Technical Program Managers, and multiple development teams
2. Responsible for achievement of Key Performance Indicators and deliverables specified by GeM
3. Partner with Business, Product / Tech owners and Operation Leaders in understanding long-term capabilities / initiatives to provide compelling capabilities for Sellers and OEMs on GeM platform that helps them succeed in their business goals
4. Based on the asks, create the product backlog and keep it groomed always
5. Identify, assess and mitigate risks, provide escalation management, anticipate and make tradeoffs balancing the business needs versus constraints
6. Clearly articulate & communicate vision, plans and project status to GeM team

8.5.2.16 Enterprise Architect

8.5.2.16.1 Qualifications

1. Master of Science/ME/MTech degree in Computer Science or related field

2. Extensive detailed working knowledge and acumen in the employment of enterprise architecture best practices, including, but not limited to, logical and physical data architectures, network communications, operating systems, applications, data base servers, application servers, web servers, server consolidation, server performance, middleware, etc.

8.5.2.16.2   Experience

1. Minimum experience of 15 years in IT with minimum 10 years' experience in enterprise architecting for large engagements.

2. Must possess experience as an enterprise architect for a completed large-scale project

3. Must have undertaken the role of Technology Architect in at least three projects

4. Experience as an application architect for at least one completed large-scale IT program

8.5.2.16.3   Roles and Responsibilities

1. Develop deep understanding of existing GeM architecture

2. Imbibe key GeM architectural principles proposed by GeM and perform detailed design of software, hardware, network and security architecture of GeM

3. Provide architectural support to MSP and solutions architects, review system designs. Work with solution architects to define solution strategy for the enterprise

4. Review software solution development to ensure alignment with the architecture designed should proactively monitor the adherence of the implementation to the chosen architecture during all iterations

5. Identify key business drivers and technology capabilities required to achieve optimum Buyer/Seller experience for GeM web and mobile apps

6. Ensure alignment between business strategies, information technology roadmap, and technical and tactical deployment teams.

8.5.2.17   Solution architect

8.5.2.17.1   Qualifications

1. Master of Science/ME/MTech degree in Computer Science / Engineering / Mathematics / Technology / Related science/technical field or related field

8.5.2.17.2 Experience

1. Minimum experience of 15 years in IT with at least 10 years' experience as an IT/ solution architect

2. Experience as an application architect for at least one completed large-scale IT program

3. Strong understanding of areas related to Service Oriented Architecture, Integration Architecture and Design Patterns, API Management etc.

8.5.2.17.3 Roles and Responsibilities

1. Develop deep understanding of existing GeM architecture and create software design plan for new GeM portal

2. Lead the design of the entire solution including systems, solutions and platforms to support GeM applications and services, including their integration with database, network, and storage solutions

3. Review software solution development to ensure alignment with the architecture designed should proactively monitor the adherence of the implementation to the chosen architecture during all iterations

4. Manage GeM platform architectural changes and ensure timely and accurate documentation of all key changes

5. Anticipate future technology requirements and recommend future state of the GeM portal architecture across the organization.

6. Proactively monitor the adherence of the implementation to the chosen architecture during all software development iterations by periodic code reviews for the new GeM portal

8.5.2.18 Security Expert

8.5.2.18.1 Qualifications

1. MCA/M. Tech/B. Tech/B.E. with a CISA/ CISSP certification

2. Master's degree in either Cybersecurity or Software engineering or related fields is preferred

8.5.2.18.2   Experience

1. Minimum of 8 years of experience in IT with minimum 5 years' experience in designing security architecture for large engagements around microservices,

2. Executed at least three projects related to design and implementation of Security Architecture

3. Technical Knowledge: UNIX, AIX, Linux, Cisco Network IDS, Host-based IDS, eTrust Access Control, ESM, and IDS. DES encryption, Digital Certificates, SSL, VPN, IPSec, TCP/IP, DNS and web security architecture, MySQL, subversion, Spam Assassin/other spam tools in a cloud environment

4. Possess extensive knowledge and experience in information technology security design, operations, encryption, information access, and

5. Strong knowledge of risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies and security attack pathologies

8.5.2.18.3   Roles and Responsibilities

1. Monitor the configuration of Security requirements of GeM cloud. Report and certify that they the design parameter as proposed in the solution and confirm to RFP requirements

2. Address key security and privacy requirements by building and tracking security metrics and designing improved security architecture for GeM portal

3. Lead all the security audits per quarter and take quick decisions on fixing up identified security threats and vulnerabilities of GeM platform

4. Participate and support application security reviews that include threat modelling, code review, and dynamic testing.

5. Support development teams in conducting security testing and other secure software development activities

8.5.2.19 Full stack developer

8.5.2.19.1 Qualifications

1. B.E. /BCA/MCA Degree in computer science
2. Proficiency in front end languages like HTML, CSS and Java script
3. Familiarity with Java script frameworks such as Angular JS, React, and Amber
4. Proficiency in server-side languages like Python, ruby, Java with microservices frameworks
5. Proficiency in microservice frameworks – spring boot, Vert.x, etc.
6. Proficiency in database technology – MYSQL, Oracle, NoSQL – MongoDB, DynamoDB

8.5.2.19.2 Experience

Should have minimum of 5 years of full stack development experience for e-commerce platforms

8.5.2.19.3 Roles and Responsibilities

1. Architect, build and maintain backend services back-end data for GeM portal using application layer, platform layer and business driven services in a microservices framework
2. Develop front end UI for GeM's micro app framework
3. Design, build and maintain high quality, reusable and reliable code for GeM based on microservices framework
4. Optimizing user experience of the GeM portal by writing code for optimizing performance, quality, and responsiveness of the GeM application
5. Identify and correct bottlenecks and fix bugs as forwarded from security or testing team

8.5.2.20 Microservices architect

8.5.2.20.1 Qualifications

1. Bachelor's degree in computer science
2. Experience with development using event-driven architecture, Test-driven development, Microservices based solutions, and Model-driven architecture is required

3. Testing – should have sound knowledge of CI/CD testing

4. Have good skills in designing API gateways for internal and external communication

8.5.2.20.2   Experience

Minimum 8 years of work experience in enterprise web application design and development with previous 4+ years' experience as an architect or technical lead role

8.5.2.20.3   Roles and Responsibilities

1. Oversee the end-to-end architecture of the new GeM portal, including its assembly and integration into the IT architecture principles while adhering to software development standards of GeM

2. Define the structure of the GeM application, its interfaces, and the principles that guide its organization, software design, and implementation and oversee development.

3. Design, develop, implement, and document test changes in microservices-based GeM application

4. Assist in the mitigation of technical risks, in order to ensure that the delivery services can be realistically delivered by the underlying technology components.

5. Monitor refactoring of GeM platform development to tackle regressions, new bugs, performance and security issues

8.5.2.21   Scrum Master

8.5.2.21.1   Qualifications

1. Bachelor's degree in computer science, agile software development/scrum master certification

2. Should be able to manage scrum teams in microservices framework

8.5.2.21.2   Experience

1. Minimum 8 years on experience in managing large functionality build with multi skilled teams preferably in an e-commerce set up

2. Extensive experience in setting up scrum boards, backlogs for the sprints

8.5.2.21.3　Roles and Responsibilities

1. Responsible for planning, monitoring, resolving dependencies across functions for deliverables against the GeM platform development

2. Lead the individual stages gates for the services, backlogs, story points and build milestones

3. Lead capacity planning, prioritization of the functionalities and scrum to scrum integration

4. Act as the single point of contact for qualified list of functionalities to be developed in a sprint by the team – works with other Scrum Masters and project managers to keep the timeline, functionalities under control

5. Ensure adoption and execution of the scrum methodology along all the project phases

8.5.2.22　Product Manager

8.5.2.22.1　Qualifications

Master's degree in management/business analysis/ organizations skills

8.5.2.22.2　Experience

Prior experience of minimum 6 years in a multi skill set up in product development, preferably in an e-commerce setup

8.5.2.22.3　Roles and Responsibilities

1. Own the GeM portal development by handling full SDLC from conceptualization to deployment of modules and entire GeM portal

2. Provide and assist software team with business requirements, roadmap compliance and ensure on-time releases for GeM applications

3. Meet regularly with all stakeholders, including product developers, marketing, customer service, finance and department heads and forward information between teams as required

4. Collect, analyze and respond to GeM platform users' feedback by planning and forwarding new feature and changes for GeM mobile and web platforms to stakeholders in GeM and MSP

5. Perform competitive analysis of similar procurement portals to propose new ideas an improvements to GeM portal for better user experience or system functionality

8.5.2.23 UI/UX experts

8.5.2.23.1 Qualifications

1. Post graduate degree in UI/UX design specifically on the web shell for micro apps

2. Should be innovative and have worked with varied stakeholders in a public sector setup

3. Proficient with visual design programs such as Adobe Photoshop and others

4. Continued education and research into UX trends and current design strategy and technologies

5. Professional written and interpersonal skills when communicating with customers and clients

8.5.2.23.2 Experience

1. Should have at least 6 years of experience in designing, conceptualizing, and producing human centered designs for web apps in the e-commerce world

2. Demonstrated Experience creating storyboards and website mapping

8.5.2.23.3 Roles and Responsibilities

1. Conduct testing of GeM application to assess user experience and ease of design

2. Use recent studies and findings to establish the best overall design elements to include in GeM portal UI

3. Build storyboards to conceptualize designs to accurately convey project plans to GeM team

4. Create surveys for research through various media platforms to gather feedback on user's ease of use and satisfaction interfacing on GeM webs and mobile app

5. Analyze customer responses and website data to examine high traffic web pages and optimize their performance

6. Enhance user experience by creating seamless navigation through various digital programs and interfaces for GeM portal

8.5.2.24 CI/CD based Unit & Integration testers

8.5.2.24.1 Qualifications

1. B.Tech / B.E. / BCA / MCA in IT / Computer Science or equivalent

2. Familiarity with build-time dependency management and unit testing and code-coverage tools

3. Knowledge of common software architectures (web/mobile/API/DB) and familiarity with REST APIs

4. Knowledge of software test life cycle activities and agile methodologies

5. Proficiency in automation tools and frameworks like Jenkins, Selenium, etc. and webservices/API testing

8.5.2.24.2   Experience

1. Minimum 4 years of experience in software testing and automation

2. Minimum 2 years automation experience with automation tools like Python, Robot, Selenium

3. Prior Experience in Functionality, Compatibility, Integration, and Regression Testing is required

8.5.2.24.3   Roles and Responsibilities

1. Anchor testing requirements , develop test plan, write test cases, execute tests and record the results for UI, Functionality, API and database testing.

2. Plan, design, code and run unit tests for new functionality on GeM portal with minimum 60% code coverage

3. Manual testing of front-end, API and back-end layers of GeM platform

4. Create accurate and concise bug reports related to the GeM portal and forward the same to the development team

5. Enable DevOps by moving code from Dev/ Test to Staging and Production. Troubleshoot issues along the CI/CD pipeline for GeM platform

6. Create automation test cases, execute tests and record results to improve GeM automation testing targets on a quarterly basis

7. Support CI/CD tools integration/ operations/ change management, and maintenance

8.5.2.25   DevOps Engineer

8.5.2.25.1   Qualifications

1. B.Sc in Any Specialization, B.Tech/B.E. in Any Specialization, BCA in Any Specialization

2. MCA in Any Specialization, M.Tech in Any Specialization, Master of Science in Any Specialization

3. Experienced in CI/CD and MS domains: configuration management and/or automation tools, and/or continuous-integration tools (like Jenkins, Git, Gitlab, BitBucket, Nexus, etc.), and/or Continuous deployment knowledge on the most popular cloud computing platforms (OpenShift, AWS, Azure and/or GCP)

4. Strong knowledge on DevOps processes and tools like Infra management, Monitoring, Security

5. Basic DB administration and performance optimization of databases

6. Aware of best practices of Application metrics like latency, availability, load etc.

8.5.2.25.2   Experience

1. Minimum 4 years of prior DevOps experience

2. Experience working in an agile development environment

3. Hands-on experience with troubleshooting of key life cycle management tools (such as BitBucket, Jenkins, Nexus, Artifactory, OCP, Sonar, AWS, Azure, GCP, etc.)

4. Hands-on experience in build, release, deployment and monitoring of cloud-based scalable distributed systems

8.5.2.25.3   Roles and Responsibilities

1. Collaborate with related Product/Account Development teams to drive automation of Configuration Management, Build, Release, Deployment and Monitoring processes, including instruction for the team on the new GeM portal

2. Support engineering and operations teams in meeting platform infrastructure needs by building, managing and automating robust CI/CD pipeline for GeM application

3. Provide professional support for the developed automations, respond to incidents to proactively prevent system outages, and ensure environments availability to meet SLAs

4. Stay up-to-date with industry best practices and contribute ideas for improvements in DevOps practices

5. Contribute to innovation through automation to enable standard deployable units of infrastructure through multiple environments until production

6. Implement security best practices to harden against all levels of security across applications, APIs, databases etc.

8.5.2.26 Pilot Deployment Specialist

8.5.2.26.1 Qualifications

1. Bachelor's in engineering/Master's degree in Computer Science or equivalent

2. Knowledge and use of automated deployment tools and solutions for full stack solutions deployment

3. Knowledge of Change Management, Release Management, Project lifecycle, and experience with planning and coordinating application deployment activities

8.5.2.26.2 Experience

1. Minimum 4 years of work experience on software deployment on application servers with preferred e-commerce platform experience

2. Familiarity and working experience with configuration and deployment of application releases on Web technologies

3. Knowledge and hands-on working experience with cloud deployment tools like Cloud AWS, DevOps tools, scripting and change management tools

8.5.2.26.3 Roles and Responsibilities

1. Own the deployment processes for both new micro services GeM application and also legacy applications to meet performance requirements of a highly scalable distributed design

2. Responsible for end-to-end launch support for pilot version releases of the GeM portal

3. Configure and deploy application releases on Web technologies (IIS, ASP, JBOSS, IBM WebSphere, and UNIX, Windows technologies

4. Configure and troubleshoot issues related to performance inefficiencies or downtime on GeM Portal

5. Responsible for building, versioning, and maintaining configuration for GeM application that needs to be deployed in different environments.

8.5.2.27   AI/ML Experts

8.5.2.27.1   Qualifications

1. Graduate / Post Graduate in Quantitative Area- B.Tech / M.Tech in CSE / Electrical / Electronic Communication/ Math Computing /Statistics /BioTech/ BioStat / Clinical Engineering in Data Science / Machine Learning

2. MBA or a Master's degree in Finance, Mathematics, Statistics, Economics, or related fields is preferred

3. Familiarity with AI disciplines in Natural Language Processing, Machine learning, Conceptual modelling, Statistical analysis, Predictive modelling, Hypothesis testing. - experience working on building an AI Conversation Voice Chatbot, NLP, Multilingual, Speech Recognition

4. Knowledge of Data Engineering Tools like MS SQL, MySQL, Oracle, etc.

5. Exposure to cloud analytics solutions and library, various data visualization tools

8.5.2.27.2   Experience

1. Minimum 6 years of strong experience in applied AI/ML/Deep Learning/Data Science

2. Deep experience in ANN /Deep Learning /Machine Learning/NLP with at least 6-8 applied AI-oriented Applied Research Projects Industry Projects applications

3. Prior exposure to Machine Learning & Quantitative Methods in Marketing / Consumer Behavior

8.5.2.27.3   Roles and Responsibilities

1. Establish KPIs, model performance metrics, identify analytical gaps, and improve performance and adoption of the GeM portal

2. Development of advanced AI/ML features for GeM portal like anomalous behaviour detection, natural language processing, etc.

3. Work closely with data scientists, engineering and other technical product/program managers to define, build, drive and measure mechanisms for optimum portal functionality

4. Identify and pitch new AI/ML use cases to GeM team based on industry best practices, trends, etc.

5. Responsible for successful deployment of GeM platform involving data pre-processing, Model Training and Evaluation, Parameter Tuning

8.5.2.28 Business Analyst

8.5.2.28.1 Qualifications

B.Tech./B.E/MCA OR Post-Graduate Degree/ Diploma in Management

8.5.2.28.2 Experience

1. Total work experience of at least 5 years with at least 2 years of e-commerce marketplace experience

2. Experience in areas such as UML, Project Management tools, Requirement Analysis and Documentation, Visio, Release Planning and Management, Budgeting, Process Mapping and Re-engineering, Six Sigma

8.5.2.28.3 Roles and Responsibilities

1. Pull data required to conduct business analysis, build reports, dashboards and metrics to monitor the performance of GeM portal

2. Assist with standards, technologies and practices for both business-to-business and business-to-consumer e-commerce models

3. Perform site performance testing and evaluation

4. Responsible for requirement gathering, business analysis and functional testing of GeM system

5. Responsible for applying their knowledge of business process modelling methodologies to document processes and present new process designs related to GeM portal to stakeholders for discussion at GeM

8.5.2.29 BI analyst cum data pipeline modeler

8.5.2.29.1 Qualifications

1. Bachelor's Degree in Business, Business Intelligence or related field is required

4. Master's Degree in Business Administration is preferred

5. Ability to understand and find appropriate applications for data and analysis results

8.5.2.29.2   Experience

Minimum experience of 5 years in a business intelligence role, designing data pipelines, ETL's for large e-commerce clients

8.5.2.29.3   Roles and Responsibilities

1. Learn and fully understand the current data landscape, BI tool framework (OLAP cubes) in GeM portal and database

2. Publish, analyze and improve GeM Seller/Buyer dashboards, operational business metrics decks and key performance indicators

3. Make recommendations for new metrics, techniques, and strategies to improve the operational efficiency and quality insight

4. Review and validate business data extracted from the GeM mobile and web apps

5. Design automated BI solutions for recurrent reporting of key metrics associated with products/services on GeM like no. of bids linked to a category, Sellers/ Service Providers associated with the category, number of contracts signed, etc.

6. Engage with GeM team to understand the needs of portal users and recommend business intelligence solutions via Seller/Buyer/OEM dashboards on GeM portal

7. Monitor analytics and KPI metrics across product and service categories on GeM portal

8. Perform product and service data profiling to identify and understand anomalies

8.5.2.30   Data migration and cutover Experts

8.5.2.30.1   Qualifications

1. Bachelor's degree in Engineering / Computer Science or similar
2. Strong data-migration design, implementation, and deployment background

3. Strong SQL scripting skills, using MS SQL Server, for both day-to-day activities and migration

4. Understanding of e-commerce domain related topics, processes and responsibilities is preferred

8.5.2.30.2   Experience

1. Minimum 10 years of experience in Data Migration, Cutover Planning, Data Analysis, Business Intelligence, Business Consulting and Project Management roles

2. Extensive Data Quality experience including cleansing and de-duplication of data

8.5.2.30.3   Roles and Responsibilities

1. Responsible for data migration and pre and post-load reporting from legacy GeM portal to new GeM portal

2. Develop test plan and testcases to demonstrate database readiness post migration

3. Identity workarounds for specific issues and corner scenarios observed during migration

4. Develop Automated/Re-usable Solutions which minimizes re-work and enables to perform rollout for future waves with minimum preparation time

5. Facilitate planning and preparation discussions to identify the detailed activities required within the cutover plan, dependencies and lead times required to execute the Cutover plan for GeM application

6. Help develop detailed cutover checklists and complete go-live readiness tasks during the Deployment phase of the GeM portal

7. Coordinate across IT and business focal points involved in testing, training and security role implementation in support of the deployment go-live

8. Post go-live, support resolution for critical defects or key risks identified during the cutover plan execution and/or during the initial start of Hypercare

8.5.2.31   Head - Legal Matters

8.5.2.31.1   Qualifications

1. Graduate/post graduate degree in Law or any other discipline related to contract management with preference for MBA

2. Strong knowledge of government policies related to public procurement, legal matters and contract management

8.5.2.31.2 Experience

1. Minimum 12 years of work experience into legal matters, with minimum of 6 years in public procurement or e-commerce industry

2. Exposure to litigation & overall judicial environment

3. Minimum 6 years' experience in Vetting, Drafting & Legal documentation with prior exposure to litigation & overall judicial environment

8.5.2.31.3 Roles and Responsibilities

1. This is a senior and a critical position and the incumbent of this position shall develop, create, and maintain policies and processes for an overall legal, secretarial, compliance and regulatory affairs program

2. Work cross-functionally and proactively to plan, direct, and drive operations to accomplish short and long term goals

3. Provide comprehensive support to GeM overall and legal team on legal & compliance issues

4. Manage relationships with regulators and government agencies with the objective to build & lead the regulatory & compliance function

5. Devise and implement legal standards, processes, systems and effective procedures to manage any legal risks associated with the GeM platform

6. Coordinate and work closely with external counsels, wherever necessary on legal advisory and litigation matters

8.5.2.32 Manager - Contract Administration

8.5.2.32.1 Qualifications

1. Bachelor's degree in Business, Accounting, or Contract Administration or equivalent experience

2. Strong negotiation skills and analytical ability

8.5.2.32.2 Experience

1. Overall 8 years of work experience in Contract & SLA management with minimum 5 years in proposal development and/or evaluation in public procurement or e-commerce industry

8.5.2.32.3   Roles and Responsibilities

1. Manage, execute, negotiate and review various types of agreements, subcontracts and other contract/legal documents with accounting, legal, program management and other organizations as necessary

2. Review and recommend contract terms and conditions to ensure adherence to GeM policy and government specifications and requirements

3. Advise management and cognizant program personnel of contractual rights and obligations

4. Interact with GeM legal department, quality, risk management, trade compliance, and sales management to ensure compliance

5. Participate in program review meetings as required and provide contract status reports for upper management review/awareness

6. Advise management of contractual rights and obligations and provides interpretations of terms and conditions of assigned program

8.5.2.33   Senior DevOps Engineer

8.5.2.33.1   Qualifications

1. B.Sc in Any Specialization, B.Tech/B.E. in Any Specialization, BCA in Any Specialization

2. MCA in Any Specialization, M.Tech in Any Specialization, Master of Science in Any Specialization

3. Experienced in CI/CD and MS domains: configuration management and/or automation tools, and/or continuous-integration tools (like Jenkins, Git, Gitlab, BitBucket, Nexus, etc.), and/or Continuous deployment knowledge on the most popular cloud computing platforms (OpenShift, AWS, Azure and/or GCP)

4. Strong knowledge on DevOps processes and tools like Infra management, Monitoring, Security

5. Basic DB administration and performance optimization of databases

6. Aware of best practices of Application metrics like latency, availability, load etc.

8.5.2.33.2   Experience

1. Minimum 7 years of prior DevOps experience

2. Experience working in an agile development environment

3. Hands-on experience with troubleshooting of key life cycle management tools (such as BitBucket, Jenkins, Nexus, Artifactory, OCP, Sonar, AWS, Azure, GCP, etc.)

4. Hands-on experience in build, release, deployment and monitoring of cloud-based scalable distributed systems

8.5.2.33.3   Roles and Responsibilities

1. Lead end-to-end DevOps activities, Pre-Production, Production deployment by managing and supporting DevOps engineers

2. Collaborate with related Product/Account Development teams to drive automation of Configuration Management, Build, Release, Deployment and Monitoring processes, including instruction for the team on the new GeM portal

3. Support engineering and operations teams in meeting platform infrastructure needs by building, managing and automating robust CI/CD pipeline for GeM application

4. Provide professional support for the developed automations, respond to incidents to proactively prevent system outages, and ensure environments availability to meet SLAs

5. Stay up-to-date with industry best practices and contribute ideas for improvements in DevOps practices

6. Contribute to innovation through automation to enable standard deployable units of infrastructure through multiple environments until production

7. Implement security best practices to harden against all levels of security across applications, APIs, databases, etc.

8.5.2.34   Chief Enterprise Architect

8.5.2.34.1   Qualifications

1. Master of Science/ME/MTech degree in Computer Science or related field

2. Extensive detailed working knowledge and acumen in the employment of enterprise architecture best practices, including, but not limited to, logical and physical data architectures, network communications, operating systems, applications, data base servers,

application servers, web servers, server consolidation, server performance, middleware, etc.

8.5.2.34.2 Experience

1. Minimum experience of 20 years in IT with minimum 15 years' experience in enterprise architecting for large engagements.

2. Must possess experience as an enterprise architect for a completed large-scale project

3. Must have undertaken the role of Technology Architect in at least three projects

4. Experience as an application architect for at least one completed large-scale IT program

8.5.2.34.3 Roles and Responsibilities

1. Manage the team providing architectural support to MSP and solutions architects, review system designs. Ensuring work is carried out with solution architects to define solution strategy for the enterprise

2. Drive the architecture and enabling technologies strategy for the infrastructure solution architecture

3. Lead architecture practice, transformation, cloud adoption, integration of IT systems

4. Develop deep understanding of existing GeM architecture

5. Imbibe key GeM architectural principles proposed by GeM and perform detailed design of software, hardware, network and security architecture of GeM

6. Review software solution development to ensure alignment with the architecture designed should proactively monitor the adherence of the implementation to the chosen architecture during all iterations

7. Identify key business drivers and technology capabilities required to achieve optimum buyer/seller experience for GeM web and mobile apps

8. Ensure alignment between business strategies, information technology roadmap, and technical and tactical deployment teams.

8.5.2.35   Senior full stack developer

8.5.2.35.1   Qualifications

1. B.E. /BCA/MCA Degree in computer science

2. Proficiency in front end languages like HTML, CSS and Java script

3. Familiarity with Java script frameworks such as Angular JS, React, and Amber

4. Proficiency in server-side languages like Python, ruby, Java with microservices frameworks

5. Proficiency in microservice frameworks – spring boot, Vert.x, etc.

6. Proficiency in database technology – MYSQL, Oracle, NoSQL – MongoDB, DynamoDB

8.5.2.35.2   Experience

Should have minimum of 7 years of full stack development experience for e-commerce platforms

8.5.2.35.3   Roles and Responsibilities

1. Manages the team and architects, builds and maintains backend services, back-end data for GeM portal using application layer, platform layer and business driven services in a microservices framework

2. Collaborate with system/feature stakeholders to discuss, collect, interpret, and analyse technical constraints and establish technical solutions

3. Develop front end UI for GeM's micro app framework

4. Design, build and maintain high quality, reusable and reliable code for GeM based on microservices framework

5. Optimize user experience of the GeM portal by writing code for optimizing performance, quality, and responsiveness of the GeM application

6. Identify and correct bottlenecks and fix bugs as forwarded from security or testing team

8.5.2.36   Integration Engineer

8.5.2.36.1   Qualifications

1. B.Tech / B.E. / BCA / MCA in IT / Computer Science or equivalent

2. Experience with programming languages like Java script, Python

3. Experience in the management of workflow tools

4. Experience in programming, IT development and computer science

8.5.2.36.2   Experience

Should have minimum of 4 years of integration engineer experience in large engagements

8.5.2.36.3   Roles and Responsibilities

1. Define integration strategies and methods and plan integrations in accordance with established deadlines and time schedules

2. Integrate new hardware and complex systems and determine whether the integration process has met GeM needs

3. Handle a broad range of software and other programming tasks to ensure that their systems integrations are functional

4. Maintain and write JavaScript-based integrations for the website.

5. Ideate, develop, and improve upon internal tooling, procedures, and processes that facilitate the work of the Technical Services team

6. Utilize internal infrastructure, tooling and documentation to solve complex, often-unique, client-specific problems

8.5.2.37   Developer – Payments

8.5.2.37.1   Qualifications

1. B.E. /BCA/MCA Degree in computer science

2. Familiar with building complex web applications using JavaScript / AJAX, XHTML, CSS.

3. Experience with or knowledge of jQuery, Java, Struts, and other website technologies.

4. Strong, object-oriented design and coding skills (C/C++ and/or Java preferably on a UNIX or Linux platform).

5. Solid software development background including design patterns, data structures, test driven development.

8.5.2.37.2   Experience

Should have 4-6 years of experience in payment operations in e-commerce, online payment system firms

8.5.2.37.3   Roles and Responsibilities

1. Handle and build payment related platform mechanisms, features and workflows for GeM

2. Design, build and maintain high quality, reusable and reliable codes for payments module for GeM with proper integrations and features

3. Optimize user experience of the GeM portal by writing code for optimizing performance, quality, and responsiveness of the GeM application

4. Take ownership of issues, investigate, conduct root-cause-analysis and resolve payment module related bottlenecks, bugs or technical issues by collaborating with payment providers, internal partners and the technology team.

8.5.2.38   Project Manager – Payments

8.5.2.38.1   Qualifications

1. B.E. /BCA/MCA Degree in computer science
2. Familiar with building complex web applications using JavaScript / AJAX, XHTML, CSS.
3. Experience with or knowledge of jQuery, Java, Struts, and other website technologies.
4. Strong, object-oriented design and coding skills (C/C++ and/or Java preferably on a UNIX or Linux platform).
5. Solid software development background including design patterns, data structures, test driven development.

8.5.2.38.2   Experience

Should have minimum 8 years of experience in payment operations in e-commerce, online payment system firms

8.5.2.38.3   Roles and Responsibilities

1. Manage the team which handles and builds payment platform mechanisms, features and workflows for GeM and keep track of regular changes and updates to be made in payment mechanisms based on new mandates from the government, policy regulations and market changes

2. Handle project management, planning, implementation progress and coordination with different stakeholders like 3P payment providers like Banks, PFMS, IFMS, etc. whenever required.

3. Take ownership of issues, investigate, conduct root-cause-analysis and resolve payments issues by collaborating with payment providers, internal partners and the technology team.

8.6 Annexure F - Service Level Requirements

8.6.1 Introduction

1. This document details the expected service levels for various services to be provided by the MSP. Performance of the MSP shall be measured against the Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) as explained and detailed in this document.

2. The service level targets define the levels of service to be provided by MSP to GeM throughout the duration of this contract or until the stated SLA targets are amended.

3. The objectives of the SLA governance model are to:

   a. Provide clear reference to service ownership, accountability, roles and/or responsibilities.

   b. Present a clear, concise and measurable description of service provisioning at each level.

   c. Match perceptions of expected service provisioning with actual service support and delivery.

4. The SLAs are intended to:

a. Make explicit the expectations that GeM has on MSP's performance throughout the duration of this project

b. Help GeM control and ensure the planned levels and performance of services

c. Trigger a process that brings GeM and MSP's management attention to some aspect of performance when that aspect drops below an agreed-upon threshold or target.

5. Refer Volume 1 Section 8.6 of this RFP for the various Services against which these service levels have been specified.

6. This is to be noted that MSP would be responsible for SLAs of any Services being provided by the sub-contractors as well. Sub-contractors' SLA would not be separate from the MSP's SLAs. MSP would be responsible for the overall delivery of services and SLAs in line with requirements of this RFP.

7. Liquidated Damages pertaining to change in the resources/ team of the MSP and delay in getting relevant certifications and standards will be levied as mentioned in Volume 1 Section 3.3.1, 3.3.3 and 7 of this RFP.

8. Liquidated Damages pertaining to delay in meeting compliance requirements will be levied as mentioned in Volume 1 Section 7 of this RFP.

8.6.2 Definitions

1. "Service Level" refers to both Key Performance Indicator and Critical Service Level.

2. "Critical Service Level" or "CSL" means a Service Level in Volume 1 Section 8.6 of this RFP that severely impacts the performance of GeM platform and hence will potentially attract Liquidated Damages.

3. "Key Performance Indicators" or "KPIs" means a Service Level in Volume 1 Section 8.6 of this RFP that is required to be monitored for GeM platform and will not attract Liquidated Damages.

4. "Expected Service Level" means

a. in respect of a Critical Service Level, the service level value pertaining to Severity Level 0 as defined in Volume 1 Section 8.6.9 of this RFP, unless otherwise specified in Volume 1 Section 8.6.9 of this RFP.

b. in respect of a Key Performance Indicator, the service level that shall be maintained as mentioned in Volume 1 Section 8.6.9 of this RFP against the KPI.

5. "At-Risk amount" shall be the quarterly fee applicable for computation of Liquidated Damages as defined in Volume 1 Section 8.6.6 of this RFP. This shall be computed as follows, pursuant to definitions provided in Volume 1 Section 6 of this RFP:

   At-Risk amount (Quarterly Fees applicable) for Implementation Phase SLAs as defined in Section 8.6.9 of Volume 1 of the RFP = Total Fixed Platform Development fee – Recoveries for payment done by GeM on behalf of MSP (if any)

   At-Risk amount (Quarterly Fees applicable) for Operations and Maintenance Phase SLAs as defined in Section 8.6.9 of Volume 1 of the RFP = Fixed O&M fee + Variable O&M fee basis confirmed orders on the GeM portal in the quarter – Recoveries for payment done by GeM on behalf of MSP (if any)

6. "Commencement Event" means "Go-Live" for all Service Levels (except implementation phase service levels that are applicable for platform development as defined in Volume 1 Section 5 of this RFP).

7. "Baseline period" refers to the period of 3 months prior to the date of applicability of different Operations and Maintenance SLA sections applicable on the new GeM platform as specified in Volume 1 Section 8.6.9.1.2 of this RFP.

8. All Critical Service Levels as mentioned in Volume 1 Section 8.6.9 of this RFP will be required to be met from Commencement Event.

9. "Measurement Period" means, in respect of any Service Level, as the period over which that Service Level is measured, calculated, and reported, or if no such period is specified, one calendar month.

10. "Severity Level" means, in respect of any Critical Service Level, degree of deviation from expected target of the Service Level.

11. "Service Level Default" is defined in Volume 1 Section 8.6.6 of this RFP.

12. "Liquidated Damages" means any amount that GeM levies on MSP for a Service Level Default with respect to a Critical Service Level pursuant to Volume 1 Section 8.6.6 of this RFP.

13. "Service Level Value" means, with respect to a Service Level, during a Measurement Period, the value of that Service Level for that Measurement Period, as calculated in accordance with Volume 1 Section 8.6.9 of this RFP.

14. "Yearly Performance" for a contract year means the average of the Service Level Values measured in each Measurement Period within that contract year.

15. "LAN" includes perimeter firewalls, IPS, NIDS, internet routers, network switches, and fibre channel switches.

16. "Servers" includes web servers, load balancer, RADIUS server, SMS gateway, messaging servers, anti-virus servers, and application servers.

17. "Storage" in this document refers to the Storage Area Network.

18. "Platform" consists of the Operating System, File System, virtualization software, RDBMS. In the case of DMZ, this also includes the Anti-virus.

19. All "days" mentioned in Volume 1 Section 8.6 of this RFP are GeM working days, "Month" will be calendar month, "quarter" a calendar quarter, "half year" a calendar half year and a "year" shall be a calendar year unless otherwise explicitly mentioned in RFP

20. "Downtime" is the time the services and facilities are not available to GeM and excludes the scheduled outages planned in advance for the Data Centre.

21. "Helpdesk Support" shall mean the helpdesk centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this project.

22. "Tickets" refers to the request generated in the Helpdesk describing the issue or problem the user is facing.

8.6.3   Measurement and Reporting

1. Volume 1 Section 8.6.9 of this RFP sets forth the Expected Service Level, Severity Level, Measurement Period, and other relevant information as applicable for each Service Level.

2. For each full Measurement Period, the MSP should obtain necessary data and calculate each of the Service Levels listed in Volume 1 Section 8.6.9 of this RFP.

3. MSP shall provision for an automated SLA management tool for efficient monitoring and processing between GeM and MSP including functionality to download system-generated

reports and supporting documents at the end of each Measurement Period, with clear calculations for each of the Service Levels listed in Volume 1 Section 8.6.9 of this RFP. Measurement methodology, tools and artefacts to be submitted shall be aligned with GeM prior to start of the Baselining Period. To this extent, possible Service Level reporting should be based on automated logs with minimal manual intervention.

4. MSP should setup and implement well-defined processes, based on mutual agreement with GeM, for Service Levels that might require manual intervention for measurement and reporting.

5. MSP should also provide detailed supporting information for the calculation of each Service Level to GeM or agency nominated by GeM, to verify the MSP's performance and compliance with each Service Level.

6. System-generated Service Level performance reports, in an agreed-upon format, should be made available in the SLA management tool. The reports should include "actual versus target" performance, severity level, variance analysis, calculation of Liquidated Damages and discussion of appropriate issues or significant events for each Service Level. Format of the reports shall be finalized by the MSP in consultation with GeM.

7. Unless a different Measurement Period is set forth in Volume 1 Section 8.6.9 of this RFP, each Service Level will be calculated on a full calendar month basis. Partial calendar month results will not be measured.

8. In the event that the measuring tools, as aligned with GeM, are not available at any time during this contract and MSP is unable to obtain sufficient data for three (3) successive Measurement Periods, the MSP shall be deemed to have failed to attain the applicable Expected Service Level for the relevant Service Level and Measurement Periods unless and to the extent that MSP can reasonably demonstrate what its actual performance was against that Service Level for the applicable Measurement Periods. For the avoidance of doubt while the MSP shall use reasonable endeavors to so demonstrate promptly there shall be no time limit on the MSP's ability to do so and if it succeeds in so doing at any time during the contract, then performance against the relevant Service Level shall be retrospectively recalculated for the purposes of the Liquidated Damages set out in this RFP to match the level of performance so demonstrated.

9. MSP shall ensure that all information, data, documentation, etc. provided by the MSP or its consortium partners (in case of consortium) or sub-contractors to GeM is accurate. In case the information, data, documentation etc. shared is found to be inaccurate, it shall be treated as an event of default and shall be governed by Volume 3 Section 13 of this RFP. In case this inaccurate information/ data/ documentation shared was used to calculate the fee payable/ already paid to the MSP, then GeM reserves the right to re-calculate the fee payable/paid to

the MSP and recover any amount paid previously over and above the re-calculated fees.

10. GeM or any third-party agency nominated by GeM reserves the right to audit the SLA management tool and related reports as it deems fit. In such cases, MSP shall provide GeM or its nominated agency access to or a copy of any information, document, data, etc. requested by GeM or its nominated agency promptly.

8.6.4   Initial Measurement Period and Baselining

8.6.4.1   Baselining Methodology

1. Before the expiry of the Baseline Period, the Parties will verify and measure each applicable Service Level, including:

    a. Expected Service Level;

    b. Measurement Period;

    c. Severity Level;

    d. Liquidated Damages pertaining to Severity Level;

    e. Measurement tools and methodologies; and

    f. Other relevant information as applicable for each Service Level

2. Following the completion of the Baselining Period, the applicable Expected Service Levels and Severity Levels shall continue to apply unless the parties agree to an adjustment, each party acting reasonably. GeM agreement shall not be unreasonably withheld where the MSP provides evidence of under or over performance root cause and effect.

8.6.4.2   Performance of the Services During Baselining

1. During the applicable Baselining Period, the MSP shall use reasonable efforts to perform the Services to the appliable Expected Service Levels set out in Volume 1 Section 8.6.9 of this RFP. However, no Service Level Defaults shall be deemed to occur during the Baselining Period in respect of such Service Levels and prior to the parties finalizing the applicable Expected Service Levels and Severity Levels thereafter.

2. Performance against any Service Levels with a Commencement Event prior to Go Live shall be evaluated to take account of the impact any Key Milestones may have upon such Service

Levels and the parties agree to revalidate the applicable Expected Service Levels alongside the completion of the final Baseline Period.

8.6.5 Service Level Default

8.6.5.1 Definition

A "Service Level Default" shall be deemed to occur with respect to a Critical Service Level for a Measurement Period if the Service Level Value for that Measurement Period is less than the applicable Expected Service Level as mentioned in Volume 1 Section 8.6.9 or this RFP.

1. Service Level Defaults shall not be attributable or deemed to occur for any Service Level which is not designated as a Critical Service Level; and

2. In circumstances where a single event results in the MSP failing to meet the Expected Service Level for more than one Critical Service Level, GeM shall select only one of those Critical Service Levels for which a Service Level Default shall be attributable or deemed to occur and for which Liquidated Damages shall accrue.

8.6.5.2 Root Cause Analysis

1. MSP shall perform an analysis to identify the root cause of failure for each instance where:

   a. In respect of Critical Service Levels, the MSP fails to meet the Expected Service Level for a Measurement Period; or

   b. In respect of Key Performance Indicators, the MSP fails to meet the Expected Service Level for the same KPI for three (3) consecutive Measurement Periods;

8.6.6 Application of Liquidated Damages

1. Liquidated Damages will be calculated quarterly based on a quarterly MSP performance evaluation conducted using the three monthly reporting periods of that quarter.

2. While SLA measurement should be done basis the Measurement period defined for each Service Level, sum of Liquidated Damages in absolute terms (in INR) associated with each Measurement Period shall apply for the applicable quarter.

   The calculation approach to be followed to arrive at the quarterly Liquidated Damages for SLAs with different Measurement Periods has been described below for reference:

a. LD Calculation for SLAs with Monthly Frequency

For a particular SLA with monthly frequency, LD should be calculated as per below mentioned process.

i. SLA percentage should be calculated on a monthly basis.

ii. As per the achieved SLA, percentage Severity should be applied for all the 3 months.

iii. As per the applied Severity, LD percentage should be applied.

iv. Final LD percentage should be calculated by taking an average of LD percentage applied for all the 3 months of a particular Quarter.

v. Final LD percentage should be considered for Quarterly MSP LD calculation.

i.e. Case 1: for System Availability SLA, parameter 1: Availability of GeM Web Portal. If the SLA achieved percentage for the 3 months is 98.7%, 99.2%,99.9%. LD calculation should be as mentioned below –

SLA Parameter		(A) SLA achieved percentage	(B) Severity	(C) LD percentage per month	(D) Final LD percentage
Availability of GeM Web Portal	*Month-1*	*98.7%*	*6*	*2%*	*(2%+1%+0%)/3 = 1%*
	Month-2	*99.2%*	*5*	*1%*	
	Month-3	*99.99%*	*0*	*0%*	

i.e. Case 2: Due to a situation, availability of help desk toll free lines went to 92% and at the same time bandwidth (MPLS lines) availability was 93% during Month-1. As it is due to same event, calculation for Month-1 should be as mentioned below:

SLA Parameter		(A) SLA achieved percentage	(B) Severity	(C) LD percentage per month
Availability of Toll Free Lines	*Month 1*	*95%*	*Sev 5 + 3% LD*	*1% + 3%* *4 % LD on this SLA Month-1*

SLA Parameter		(A) SLA achieved percentage	(B) Severity	(C) LD percentage per month
Availability of Bandwidth	Month 1	95.5%	Sev 6 + 2.5% LD	1% + 2.5% 3.5% on this SLA for Month-1

As per above mentioned calculation, additional LD applicable on MSP is (3%+ 2.5%) = 5.5% > 5%. As mentioned, in case of additional LD clauses in Volume 1 Section 8.6.9 of the RFP, maximum applicable LD is 5%. Final LD calculation should be as mentioned below:

SLA Parameter		(A) SLA achieved percentage	(B) Severity	(C) LD percentage per month
Availability of Toll Free Lines	Month 1	95%	Sev 5 + 3% LD	1% + 5% 6% LD on this SLA for Month-1
Availability of Bandwidth	Month 1	95.5%	Sev 6 + 2.5% LD	1% LD on this SLA for Month-1 (2.5% applicable LD as per SLA adjusted with above SLA as 5% is max. additional LD)

LD on Month-2 & Month-3 should be calculated applying the same logic as per SLA achieved percentage of that particular month. Final LD percentage should be calculated by taking an average of LD percentage applied for all the 3 months of a particular Quarter. The Final LD percentage shall be considered for Quarterly MSP LD calculation.

b. **LD Calculation for SLAs with quarterly/ half-yearly/ yearly frequency**

For a particular SLA with quarterly/ half-yearly/ yearly frequency, LD should be calculated as per below mentioned process.

   i.   SLA percentage should be calculated on a particular Quarter, based on the

status of activity and closure of all such activity as per defined cycle/ timeline (if any)

ii.   As per the achieved SLA, percentage Severity should be applied.

iii.   As per the applied Severity, LD percentage should be applied. The same LD should be considered as Final LD percentage of a particular Quarter.

iv.   Final LD percentage should be considered for Quarterly MSP LD calculation.

i.e. Case 1: for Cloud Service parameter 4: DC-DR Drill. If the SLA is achieved for the quarter as drills are conducted as per schedule. LD calculation should be as mentioned below:

SLA Parameter		(A) SLA achieved percentage	(B) Severity	(C) LD percentage per month	(D) Final LD percentage
DC-DR Drill	Quarter	100% (2 Drills conducted as per schedule)	0	0%	0%

3.   Breach of Expected Service Levels shall result in various Severity Levels based on the business impact caused by each Service component to GeM operations. The Severity Levels and the associated financial Liquidated Damages are defined as below:

Severity Level	Liquidated Damages *(as a percentage of At-Risk amount applicable for Operations & Maintenance SLAs as defined in Volume 1 Section 8.6.2 of the RFP)*
9	Event of default and termination as per Volume 3 Section 13 of this RFP and the corresponding consequences shall follow
8	5.0%
7	4.0%
6	2.0%
5	1.0%
4	0.5%

3	0.4%
2	0.2%
1	0.1%
0	Expected service level; No Liquidated Damages applicable

Table 115: Severity Levels and Liquidated Damages

4. In no event will the aggregate amount of Liquidated Damages levied with respect to all Service Level Defaults in a quarter exceed 20% of Total At-Risk amount for that quarter. However, other Liquidated Damages/ deductions as defined in the RFP, such as LDs pertaining to resource replacement and delay in meeting compliance requirements, shall be levied over and above the 20% cap as mentioned in Volume 1 Section 3.3.3 and 3.3.4, and Section 7 of this RFP.

5. If Liquidated Damages exceed 20% of the At-Risk amount for 6 (Six) consecutive quarters, then GeM reserves the right to take appropriate action including termination of the contract and forfeiting of Performance Bank Guarantee.

6. The Parties agree that any liquidated damages levied under this Agreement do not constitute a penalty and that the Parties, having negotiated in good faith for such specific liquidated damages and having agreed that the amount of such liquidated damages is reasonable in light of the anticipated harm and loss caused by the breach related thereto and the difficulties of proof of loss and inconvenience or non-feasibility of obtaining any adequate remedy, are stopped from contesting the validity or enforceability of such liquidated damages.

8.6.7 Administration of Service Level Agreements

1. This document defines the following management procedures:

   a. An issue management process for documenting and resolving particularly difficult issues.

   b. GeM and MSP's management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

8.6.7.1 Issue Management Process

8.6.7.1.1 General

1. This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between GeM and MSP. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

8.6.7.1.2 Issue management process

1. Either GeM or MSP may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

2. GeM and MSP's representative will determine which committee or executive level should logically be involved in resolution. A chain of management escalation is to be defined based on mutual agreement between GeM and MSP.

3. GeM and MSP Management will develop a temporary, if needed, and the permanent solution for the problem at hand. MSP will then communicate the resolution to all interested parties.

4. In the event a significant business issue is still unresolved, the arbitration procedures described in the Contract will be used.

8.6.7.2 Management escalation procedures and contact map

1. The purpose of this escalation process is to provide a quick and orderly method of notifying

both parties that an issue is not being successfully resolved. Implementing this procedure ensures that GeM and MSP's management are communicating at the appropriate levels.

2. Escalation should take place on an exception basis and only if successful issue resolution cannot be achieved in a reasonable time frame.

   a. Either GeM or MSP can initiate the procedure

   b. The "moving party" should promptly notify the other party that management escalation will be initiated

   c. Escalation matrix to be defined in mutual agreement between GeM and MSP

   d. Escalation will be one level at a time and concurrently

8.6.8   Service Levels for a New Service or Additional Service

1. With respect to a New Service or Additional Service, MSP and GeM will establish initial Service Levels following full implementation of such Services which will apply during the initial 90-day period of MSP providing such New Service or Additional Service.

2. To the extent appropriate, such initial Service Levels will be the same as or similar to existing Service Levels for the same or similar Services.

3. During such 90 days, MSP and GeM will conduct a process for Measurement of Service Levels to validate the initial Service Levels and agree upon the actual Service Levels.

4. The finalized service levels shall be documented and implemented in adherence with the SLA version control process.

8.6.9 APPENDIX I

8.6.9.1 Service Levels Table

8.6.9.1.1 Implementation phase SLAs

The Implementation Phase SLAs shall be applicable from the date of signing of the Agreement till the Go-live of new GeM platform.

#	Measurement	Definition	Service Level value	Liquidated Damages *(as a % of Total Fixed Platform Development fee as defined in Volume 1 Section 6 of this RFP)*
1	Team mobilization and commencement of work	1. Mobilization & deployment of Key Resources, as defined in Volume 2 Section 2.3 of this RFP, for commencement of work. Commencement of work would mean reporting of MSP's Key Resources at GeM Office for project planning and kick-off. 2. For delay of each additional week or part thereof after 60 days, 0.1% of Total Fixed Platform Development fee shall be levied as additional Liquidated Damages.	<=21 Days	Nil
			> 21 days & <= 45 days	0.05%
			> 45 days & <= 60 days	0.1%
			> 45 days & <= 60 days	0.2%

#	Measurement	Definition	Service Level value	Liquidated Damages *(as a % of Total Fixed Platform Development fee as defined in Volume 1 Section 6 of this RFP)*
2	Project Planning	1. Submission of a detailed implementation Project Plan including design, core development, acceptance testing phases, resource deployment plan and Communication Framework 2. For delay of each additional week or part thereof after 120 days, 0.1% of Total Fixed Platform Development fee shall be levied as additional Liquidated Damages.	<=60 Days	Nil
			> 60 days & <= 90 days	0.4%
			> 90 days & <= 120 days	1%
3	Delay in any of the project milestones #3 to #8 as defined in Volume 1 Section 5 of this RFP	3. Measured as the difference between the planned date for the milestone and the actual date of its completion 4. For delay of each additional week or part thereof after 20 days, 0.05% of Annual fixed O&M fee shall be levied as additional Liquidated Damages.	< 10 days	Nil
			> 10 days & <= 15 days	0.1%
			> 15 days & <= 20 days	0.15%
4	Delay in overall Go- Live date	1. Measured as the difference between the planned date for the Go-Live and the actual date of Go-Live 2. For delay of each additional week or part thereof after 25 days, 0.5% of Total Fixed Platform	< 10 days	Nil
			> 10 days & <= 15 days	0.5%
			> 15 days & <= 20 days	1%
			> 20 days & <= 25 days	1.5%

#	Measurement	Definition	Service Level value	Liquidated Damages *(as a % of Total Fixed Platform Development fee as defined in Volume 1 Section 6 of this RFP)*
		Development fee shall be levied as additional Liquidated Damages.		

8.6.9.1.2   Operations and Maintenance phase SLAs

The Operations and Maintenance SLAs shall be applicable as per timelines mentioned below:

#	SLA Section	Date of Applicability
1	Systems availability SLA	6 months post current platform handover, i.e., 1st Jul 2024 onwards
2	Performance SLAs	6 months post current platform handover, i.e., 1st Jul 2024 onwards
3	Reporting SLAs	6 months post current platform handover, i.e., 1st Jul 2024 onwards
4	Cloud Services SLAs	6 months post current platform handover, i.e., 1st Jul 2024 onwards
5	Audit SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards
6	Security SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards

#	SLA Section	Date of Applicability
7	Helpdesk and Contact Center SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards
8	Service Management SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards
9	Change Management SLAs	6 months post current platform handover, i.e., 1st Jul 2024 onwards
10	Project Management SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards
11	Business Services SLAs	From the expiry of current contract, i.e. 1st Jan 2024 onwards

During the 6 (six) month period between handover of the current GeM platform from the outgoing MSP and Go-Live of the new platform, the existing SLAs applicable on the current GeM platform, as mentioned in Section 8.6.10 of Volume 1 of the RFP, should continue to apply to the incoming MSP. The performance levels pertaining to these SLAs shall be re-calibrated to the average performance levels recorded in the last two quarters of the outgoing MSP's contract period, i.e., from 1st July'23 to 31st December'23. However, GeM may at its sole discretion, waive off the LD in this case, wherein in the opinion of GeM, there are adequate reasons to justify that the breach of SLAs were due to reasons not within the control of the MSP.

Systems availability SLA

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Availability of GeM Web Portal	% of Uptime for GeM Web Portal **Metric:** % of Uptime for GeM Web Portal **Formula:** Uptime % = (1-[(Total Downtime) / (Total Time – Planned Downtime)]) *100	**Service Level Type** : CSL	>=99.99%	0
				<99.99% and >= 99.9%	3

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		GeM web portal is expected to be available 24 x 7. **Total Downtime -** Total cumulative time the GeM Web portal is NOT available. **Planned Downtime -**Total maintenance time as defined and agreed upon by MSP and GeM. **Total Time -** 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment/ At-Risk amount shall be levied as additional Liquidated Damages with a maximum cap of 5%	**Frequency:** Monthly	<99.9% and >= 99.5%	4
				<99.5% and >= 99.0%	5
				<99.0% and >= 98.5%	6
				<98.5% and >= 98.0%	7
				<98.0%	8
2	Availability of the below mentioned 5 (five) critical Services of the GeM System *(as defined in Volume 1 Section 8.1 & 8.2 of this RFP)*: 1. E-Procurement 2. Registration 3. Category Management 4. Catalogue Management	The availability of the mentioned five (05) critical Services & Functionalities of the GeM System measured as % uptime **Metric:** % of Uptime **Formula:** Uptime % = (1-[(Total Downtime) / (Total Time – Planned Downtime)]) *100 GeM Services – All Modules are expected to be available 24 x 7. **Total Downtime -** Total cumulative time the mentioned GeM Services & Functionalities are NOT Available.	**Service Level Type** : CSL **Frequency:** Monthly	>=99.99%	0
				<99.99% and >= 99.9%	3
				<99.9% and >= 99.5%	4
				<99.5% and >= 99.0%	5
				<99.0% and >= 98.5%	6

#	Category/ Component	Definition	Information	Service Level value	Severity Level
	5. SSO/ARX *GeM reserves the right to change the above services & functionalities as per business requirements	**Planned Downtime -**Total maintenance time as defined and agreed upon by MSP and GeM. **Total Time -** 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages with a maximum cap of 5%		<98.5% and >= 98.0%	7
				<98.0%	8
3	Availability of other critical Services *(as defined in Volume 1 Section 8.1 & 8.2 of this RFP)* 1. Contract Management 2. Learning Management System 3. Order Fulfillment 4. Analytics & Business Intelligence 5. Payments 6. Administration 7. Incident Management 8. Assets BG 9. Assets MKP	The availability of the mentioned 10 Services & Functionalities of the GeM System measured as % uptime **Metric:** % of Uptime **Formula:** Uptime % = (1-[(Total Downtime) / (Total Time – Planned Downtime)]) *100 GeM Services – All Modules are expected to be available 24 x 7. **Total Downtime -** Total cumulative time the mentioned GeM Services & Functionalities are NOT Available. **Planned Downtime -**Total maintenance time as defined and agreed upon by MSP and GeM. **Total Time -** 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly	**Service Level Type** : CSL **Frequency:** Monthly	>=99.99%	0
				<99.99% and >= 99.9%	1
				<99.9% and >= 99.5%	2
				<99.5% and >= 99.0%	3
				<99.0% and >= 98.5%	4
				<98.5% and >= 98.0%	5
				<98.0%	6

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Payment shall be levied as additional Liquidated Damages with a maximum cap of 5%			
4	Availability of Bandwidth (Internet and WAN MPLS)	GeM System Availability over MPLS / Internet

For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages with a maximum cap of 5% | **Service Level Type** : CSL

Frequency: Monthly | >= 99.99% | 0 |
				<99.99% and >= 99.9%	1
				<99.99% and >= 99.5%	2
				<99.5% and >= 99.0%	3
				<99.0% and >= 98.5%	4
				<98.5% and >= 98.0%	5
				<98.0%	6

Performance SLAs

#	Category/Component	Definition	Information	Service Level value	Severity Level
1	Average page loading time for all services	Page loading time measured Monthly. *The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR. Exact URLs for measurement of performance SLAs to be finalized mutually between GeM and MSP during design phase.*	**Service Level Type:** CSL **Frequency:** Monthly	>=98% within the limit of 2 seconds	0
				<98% and >=95% within the limit of 2 seconds	1
				Less than 95% within the limit of 2 seconds	2
2	Transaction response time except the transactions mentioned in row 3 below.	Response time of services measured monthly *The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR. Exact URLs for measurement of performance SLAs to be finalized mutually between GeM and MSP during design phase*	**Service Level Type** : CSL **Frequency:** Monthly	>=99% within the limit of 2 seconds	0
				<99% and >=96% within the limit of 2 seconds	1
				Less than 95% within the limit of 2 seconds	2
3	Transaction response time involving uploading/ downloading of documents (avg. size 2 MB)	Response time of services measured monthly *The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR. Exact URLs for measurement of performance SLAs to be finalized mutually between GeM and MSP during design phase*	**Service Level Type**: CSL **Frequency:** Monthly	>=98% within the limit of 5 seconds	0
				<98% and >=95% within the limit of 5 seconds	1
				Less than 95% within the limit of 2 seconds	2

Reporting SLAs

#	Category/Component	Definition	Information	Service Level value	Severity Level
1	Standard Reports Publishing	Adherence to publishing of standard reports within the defined time and agreed frequency *(as aligned with GeM during design phase).*	**Service Level Type:** CSL **Frequency:** Monthly	<12 hours	0
				Between 12-24 hours	2
				<24 hours	4
2	Average Response time for Self Service reports	Time taken to generate self- service reports that are available in the Analytics & BI tool.	**Service Level Type:** KPI **Frequency:** Monthly	>90% in <20 seconds	N/A

Cloud services SLAs

#	Category/Component	Definition	Information	Service Level value		Security Level
1	Recovery Time Objective (RTO)	Based on the successful operations from DR Site and restoring the services back For delay of each additional 2 Hours or part thereof after 6 Hours, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages with a maximum cap of 5%	**Service Level Type :** CSL **Frequency:** As per defined DC-DR Drill frequency	< 2 Hours	0	
				2-4 Hours	5	
				4-6 Hours	7	
				>6 Hours	8	
2	Recovery Point Objective (RPO)	Based on the successful operations from DR Site and restoring the services back. For delay of each additional 30 minutes or part thereof after 90 minutes, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages with a maximum cap of 5%	**Service Level Type :** CSL **Frequency:** As per defined DC-DR Drill frequency	< 30 Mins	0	
				30-60 Mins	5	
				60-90 Mins	7	
				> 90 Mins	8	
3	Provisioning and deprovisioning of Virtual Machines/ Containers/ Alternates	Per Occurrence. This will be calculated monthly. For delay of each additional 30 minutes or part thereof after 45 minutes, additional 0.5% of the	**Service Level Type :** CSL **Frequency:** Monthly	<15 Mins	0	
				15-45 Mins	6	

#	Category/Component	Definition	Information	Service Level value	Security Level
		Quarterly Payment shall be levied as additional Liquidated Damages with a maximum cap of 5%			
4	DC-DR Drill	Number of Drills as per the defined Policy OR at least 2 DR Drills in a year (once every 6 months) This will be measured every 6 months and the Liquidated Damages will be levied in the quarter following the end of the six month period.	**Service Level Type :** CSL **Frequency:** As per defined DC-DR Drill frequency	2 Drill	0
				1 Drill	5
				0 Drills	6
7	Spinning up Object Storage (once approval for the same has been granted)	Time to spin up Object Storage	**Service Level Type**: KPI **Frequency:** Monthly	>=95% in <4 hours	N/A
8	OS Currency	Application workload per cent on (N-1) or better	**Service Level Type**: KPI **Frequency:** Half-yearly	>=95%	N/A
9	Advise client of Potential Need to Allocate Additional Processing	Parameter to measure the timely notification of the need to allocate additional processing resources based on predefined parameters and observed growth patterns. **Metric** = Upon sustained average during 30min	**Service Level Type:** KPI **Frequency:** Monthly	>=99%	N/A

#	Category/Component	Definition	Information	Service Level value	Security Level
		CPU/Memory utilization exceeding 90% of installed processor capacity, MSP will inform GeM within one elapsed day of the over 90% capacity situation. **Formula:** Number of completed occurrences within the time during measurement interval / Total number of occurrences during a measurement interval **Percent (%) CPU/memory utilization** = [CPU/memory time in use completed within target performance during the measurement interval] divided by [Total available CPU/memory required to be performed by External Service Provider during the measurement interval]			

#	Category/Component	Definition	Information	Service Level value	Security Level
10	On-Demand CPU/memory Processing Capability Change Requests	Parameter to measure the timely increase or decrease of CPU/memory processing capability upon receipt of a change request from the client. **Metric:** Upon request from a client requesting that CPU/memory processing capability be increased or decreased by any percentage within 20% of current CPU processing capability, MSP will complete such change within 8 hour of Change Request. **Formula:** Time is measured from receipt of the approved change request from GeM to the completion of the request	**Service Level Type:** KPI **Frequency:** Monthly	>=99%	N/A
11	Advise client of Potential Need to Allocate Additional Storage	Parameter to measure the timely notification to the client of the potential need to allocate additional storage resources based on predefined parameters and observed growth patterns. Time is measured from when the total monthly storage capacity utilization (measured in GBs used) exceeds 85% of installed capacity **Metric:** Upon total monthly storage capacity utilization exceeding 85% of installed capacity,	**Frequency:** Monthly **Service Level Type:** KPI	>=99%	N/A

#	Category/Component	Definition	Information	Service Level value	Security Level
		MSP will inform GeM of the need to increase capacity within one elapsed day **Formula:** Number of completed occurrences within the time during measurement interval/ Total number of occurrences during the measurement interval **Percent (%) storage utilization:** [storage in use completed within target performance during the measurement interval] divided by [Total available storage required to be performed by External Service Provider during the measurement interval]			
12	On-Demand Storage Capacity Change Requests	Parameter to measure the timely completion of each increase or decrease in storage capacity as scheduled under the change management process. **Metric:** Upon request from a client requesting that installed storage capacity be increased or decreased by any percentage within 10% of then-current installed Storage capacity, MSP will complete such change within 4 hours of the Change Request.	**Service Level Type:** KPI **Frequency:** Monthly	>=99%	N/A

#	Category/Component	Definition	Information	Service Level value	Security Level
		Formula: Number of completed occurrences within the time during measurement interval/ Total number of occurrences during the measurement interval Time is measured from receipt of the authorized change request from GeM to the completion of the request			
13	Adherence to Backup Policy	Based on the backup policy of GeM. 100% backups shipped to offsite location on schedule in accordance with the GeM's Backup Policy. 100% backup restoration testing on time in accordance with the GeM's Backup Policy.	**Service Level Type:** CSL **Frequency:** Monthly	100% backup on time as per backup policy	0
				< 100% backup restoration testing on time in accordance with the GeM's Backup Policy	3
				< 100% backups shipped to offsite location on schedule in accordance with the GeM's Backup Policy	4
				< 100% backups taken on time as per the GeM's Backup Policy	5

Audit SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Outcome of Half Yearly IT Security Audit	The third-party auditor shall rate the performance of the MSP on IT Security implementation. The three ratings for the performance shall be: Satisfactory, Requires Improvement and Unsatisfactory *Appointing a 3rd party Auditor is the responsibility of GeM. MSP's support to GeM for external audits shall be considered in this category.* *GeM to notify MSP before initiating the audit if the same will be considered for this SLA measurement.*	**Service Level Type**: CSL **Frequency:** Half Yearly	Satisfactory	0
				Requires Improvement rating	5
				Unsatisfactory rating	6

#	Category/ Component	Definition	Information	Service Level value	Severity Level
2	Implementation of recommendations of previous IT Security audits	Implementation of recommendations given by the IT Security auditor and which have been agreed upon to be implemented by MSP and GeM. *Timeline for implementation of each recommendation to be mutually agreed between GeM and MSP. Any recommendation from Security auditor shall be taken in this regard.*	**Service Level Type**: CSL **Frequency:** As per Audit	100% on Time	0
				<100% on Time	5

Security SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Security reporting	100% reporting of the predefined security KPIs within predefined timelines. MIS report to be submitted on quarterly basis. ***List of minimum Security KPIs to be measured for this Service Level is provided below.*	**Service Level Type:** CSL **Frequency:** Quarterly	On Time	0
				> 1 day & <= 5 days delay	4
				> 5 day & <= 10 days delay	5
				> 10 day & <= 15 days delay	6
				> 15 days delay	7
2	Patch updates			>=98%	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Availability of latest patches on the system components. All patches released, to be installed on at least 98% of all applicable components as per Patching policy.	**Service Level Type:** CSL **Frequency:** Quarterly	>= 97% & < 98%	4
				>= 96% & < 97%	5
				>= 95% & < 96%	6
				<95%	7
3	Anti-Virus (AV) Signature Update	Availability of latest AV signature on the system components. Latest AV signature to be installed on at least 98% of all applicable components within 24 hours.	**Service Level Type:** CSL **Frequency:** Quarterly	>=98%	0
				>= 97% & < 98%	4
				>= 96% & < 97%	5
				>= 95% & < 96%	6
				<95%	7
4	Vulnerability assessment and closure (scope to be defined at project start)	Vulnerability Assessment for all systems / subsystems / network devices shall be performed once every six months and all detected vulnerabilities shall be closed within the same cycle.	**Service Level Type:** CSL **Frequency:** Half-yearly	<=10 days	0
				>10 and <=20 days	4
				>20 and <=30 days	5
				>30 and <=35 days	6
				>35 days	7

#	Category/ Component	Definition	Information	Service Level value	Severity Level
5	Penetration testing	Penetration Testing (external) will be conducted once every quarter. All detected vulnerabilities to be closed within the year.	**Service Level Type** : CSL **Frequency:** Yearly	<=10 days	0
				>10 and <=30 days	4
				>30 and <=40 days	5
				>40 and <=45 days	6
				>45 days	7
6	Reporting of Security Incidents	Detecting and reporting of security incidents/ threats within 15 minutes of detection. For delay of each additional 1 hour or part thereof after 1 hour, additional 0.05% of the Quarterly Payment shall be levied as additional Liquidated Damages.	**Service Level Type:** CSL **Frequency:** Quarterly	100% incidents reported within 15 minutes	0
				100% incidents reported within 30 minutes	4
				100% incidents reported within 1 hour	5

**List of Security KPIs to be measured for "Security Reporting" Service Level:

Security KPI	Frequency	Method of measurement
Count of Critical Vulnerabilities which are open for more than 3 months.	Monthly	Run a VA report after 90 days and count number of vulnerabilities common between two runs on same servers.

No of users having PIM access without Proper Approval	Monthly	PIM reconciliation report review by security team.
Security Exceptions – Count of Security Exceptions open for that month	Monthly	Total number of open exceptions in the security area.
No of Firewall rules implemented without proper approval	Monthly	Firewall reconciliation report review by security team.
Count of Irrelevant Rules configured in SIEM	Monthly	Review of SIEM rules and feedback on that only relevant rules are implemented. Additional rules can be modified / implemented as required
No of users having VPN access without Proper Approval	Monthly	VPN User reconciliation report review by security team.
Daily AV Compliance	Daily	(Count of Servers where AV signature not getting updated on Daily basis + Count of Servers which have documented exception approval)/ (Total Count of Production Servers)
Monthly AV Compliance	Monthly	(Count of Servers where AV signature not getting updated on Daily basis + Count of Servers which have documented exception approval)/ (Total Count of Production Servers)

Helpdesk and Contact Centre SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Availability of Toll-Free Lines	Downtime shall be measured from the time the Toll Free Line at a help desk becomes unavailable to the end users to the time it becomes available to end users s hours to be 9:00 AM to 10:00 PM each day for 6 days a week (Monday – Saturday). (Working hours and days are subject to change as per GeM's requirements) Downtime is to be calculated by measuring difference between start time and end time for failure incidents of toll free lines during helpdesk working hours for that month. **Calculation:** Uptime = (1 - [[(Toll Free Line downtime) / (Total Time)]]) e.g., if there are 26 helpdesk working days in a month, and the link was down on day one from 1 pm to 3 pm, and on day two from 5 pm to 9 pm and there was no downtime after that then Total down time is (2 hours from day 1 and 1 hour from day 2 = 3 hours).	**Service Level Type:** CSL **Frequency:** Monthly	>=99.5% uptime of all the toll-free lines	0
				>= 99.0% to < 99.5% uptime of all the toll-free lines	3
				>= 98.5% to < 99.0% uptime of all the toll-free lines	4

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Total time is 26x9=234 hours. Uptime = 1 - (3/234) = 0.9873 = 98.73% For each additional drop of 1% in performance below 98%, additional 1% of the Quarterly Payment shall be levied as additional Liquidated Damages with maximum cap of 5%.		>= 98.0% to < 98.5% uptime of all the toll-free lines	5
2	Call Queue Waiting time	Call queue waiting time is the waiting time in Automatic Call Distributor (ACD) queue after pressing the prescribed digit to talk to the agent but before being answered by the agent. Abandoned Calls within 5 seconds not to be considered in target. **Metric:** Measured as % of calls where 'call queue waiting time' is less than 20 seconds.	**Service Level Type:** CSL **Frequency:** Monthly	>=90% calls with waiting time within 20 seconds	0
				>=89% and <90% calls with waiting time within 20 seconds	1

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Calculation: Call Queue Waiting time = Calls answered within 20 seconds/(Calls offered - Calls abandoned within 5 seconds). For each additional drop of 1% in performance below 90%, additional 1% of the Quarterly Payment shall be levied as additional Liquidated Damages with maximum cap of 5%.		>=88% and <89% calls with waiting time within 20 seconds	2
				>=87% and <88% calls with waiting time within 20 seconds	3
				>=86% and <87% calls with waiting time within 20 seconds	4
				<86% calls with waiting time within 20 seconds	5
3	Helpdesk Ticket Response time	Time taken to acknowledge and respond once a Ticket is logged through either Email OR Web tickets. This is to be calculated for all Tickets reported within the reporting month.	**Service Level Type:** CSL	>=99% Tickets within 15 minutes	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		For each additional drop of 1% in performance below 95%, additional 1% of the Quarterly Payment shall be as additional Liquidated Damages with maximum cap of 5%.	**Frequency:** Monthly	>=98% and <99% Tickets within 15 minutes	4
				>=96% and <98% Tickets within 15 minutes	5
				>=95% and <96% Tickets within 15 minutes	6
4	Escalation Desk Resolution Rate	**Metric:** Rate of resolution of the Ticket logged through escalation desk (emails received to support.gem@gov.in, Social Media and escalated on the GeM portal) **Calculation**: Escalation Desk Resolution Rate = (Total Number of escalation desk Tickets resolved within 16 working hours for the	**Service Level Type:** CSL **Frequency:** Monthly	>=95% within 16 working hours	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		month) / (Total Number of escalation desk Tickets received for the month) Daily follow ups to be done (excluding Sundays & Holidays) with concerned parties. Verified by random audit on 10% sample and MSP to ensure >90% compliance. Random sampler and data selection shall be by GeM. For each additional drop of 1% in performance below 95%, additional 1% of the Quarterly Payment shall be levied as additional Liquidated Damages with maximum cap of 5%.		>=93% and <95% within 16 working hours	4
				>=90% and <93% within 16 working hours	5
				<90% within 16 working hours	6
5	CSAT	CSAT shall be calculated based on the score the customer gives in the range of 1 to 5.	**Service Level Type:** CSL	>=82% CSAT and Trigger rate >=99%	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Trigger is when an agent attempts to the User requesting to participate in the CSAT survey on IVR **Calculation**: CSAT = (Total count of Excellent responses [5]+ Total count of Very Good responses[4])/(Total Count of Responses) Trigger Rate = Basis Random Audits of 1000 samples. MSP to ensure >90% compliance. (Random sampler and data selection shall be through mutual consent)	**Frequency:** Monthly	>= 80% and <81.99% CSAT; and Trigger rate >=99%	3
				<80% CSAT and Trigger rate >=99%	4
		For each additional drop of 1% in performance below 80% in case of CSAT and below 90% in case of trigger rate, additional 1% of the Quarterly Payment shall be levied as additional Liquidated Damages with maximum cap of 5%.			
6	Time to resolve Tickets	Time taken to resolve the reported problem in all Tickets, except escalation Desk Tickets. **Calculation Method**: Time to resolve = (Total number of Tickets resolved within 16 hours for	**Service Level Type:** CSL **Frequency:** Monthly	>=98% within 16 working hours	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		the month) / (Total Number of Tickets created for that month) Good amount of follow ups per week to be done with external parties (for tickets depending on 3rd Party/GeM/End Customer). SoP to be created by MSP and approved by GeM. GeM to perform Random Samples for verification. For each additional drop of 1% in performance below 95%, additional 1% of the Quarterly Payment shall be levied as Liquidated Damages with maximum cap of 5%.		>=97% and <98% within 16 working hours	2
				>=96% and <97% within 16 working hours	3
				>=95% and <96% within 16 working hours	4
7	Percentage of reopened Tickets	For all Tickets which are designated resolved by the agent but are re-opened by the customer for the month. This is calculated for all Tickets reported within the month.	**Service Level Type:** CSL **Frequency:** Monthly	<=2% Tickets	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		Calculation: Percentage of reopened Tickets = (Total Number of Tickets reopened by client within 7 days after Ticket was set to resolved status) / (Total number of Tickets for the month**.** For each additional increase of 1% in tickets above 8%, additional 1% of the Quarterly Payment shall be levied as additional Liquidated Damages with maximum cap of 5%.		>2% and <=4% tickets	5
				>4% and <=6% tickets	6
				>6% and <=8% tickets	7
8	FCR (First Contact Resolution)	First Contact Resolution rate is the percentage of customers who got their issue resolved within their touchpoint interaction on the first call or contact. **Calculation**: FCR **=** Summation for every working day of the month (Total number of unique calls answered for every calendar day) /	**Service Level Type:** CSL **Frequency:** Monthly	>=80%	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
		(Total number of calls answered for that calendar day) For each additional drop of 1% in performance below 78%, additional 1% of the Quarterly Payment shall be levied as Liquidated Damages with maximum cap of 5%.		<80% and >=78%	3
				<78% and >=75%	4
				<75%	5
10	Performance Quality	Quality Management System to be followed. Quality scores at all desks should be >=90%. *The parameters & mechanism for calculating quality score will be defined by GeM.* Audits will be done by MSP team and sample for the audit will be provided by GeM.	**Service Level Type:** CSL **Frequency:** Monthly	>=90%	0
				>=85% and <90%	3
				<85%	4

#	Category/ Component	Definition	Information	Service Level value	Severity Level
11	Inbound calls abandonment rate	Call abandonment rate (unanswered calls by helpdesk agents) This measures % of calls that were requested for an agent but got disconnected before being answered by the agent. Only calls that get disconnected after 20 seconds from transfer using IVRS options will be considered for computation of this SLA.	**Service Level Type:** KPI **Frequency:** Monthly	<=2%	N/A
12	Agent Utilization Rate	[(Average Number of Handled Calls) x (Average Handling Time)] ÷ [(Total Work Hours in Given Period) x 100**%]**	**Service Level Type:** KPI **Frequency:** Monthly	>=90%	N/A
13	Agent Attrition Rate	(Number of Employees that Left during A Given Period) ÷ (Average Number of Employees for the Period) × 100**%**	**Service Level Type:** KPI **Frequency:** Monthly	<8%	N/A

Service Management SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Service Management (SIAM) - On-Time Delivery of SIAM Reports	By the 10th calendar day of the month following the reporting period.	**Service Level Type**: KPI **Frequency**: Monthly	>= 95%	N/A
2	Service Management (SIAM) - Time taken to open a Major Incident bridge	**Calculation:** (Number of instances with <=15 minutes time taken to open a Major Incident bridge) / (Total Number of instances wherein Major Incident bridge was opened)	**Service Level Type**: KPI **Frequency**: Monthly	>= 95%	N/A
3	Service Management (SIAM) - On-time occurrence of Major Incident Review of S1 Incidents	**Calculation:** (Number of S1 incidents with review in <= 2 Business Days after S1 Incident is resolved) / (Total Number of S1 incidents) in the measurement period	**Service Level Type**: KPI **Frequency**: Monthly	>= 95%	N/A
4	Service Management (SIAM) - On-time occurrence of Post Implementation Review for failed Changes	**Calculation:** (Number of instances with review in <= 2 Business Days after a Failed Change is identified) / (Total Number Failed Change identified) in the measurement period	**Service Level Type**: KPI **Frequency**: Monthly	>= 95%	N/A
5	Response time for a Severity 1 (S1) incident	Average Time is taken to acknowledge and respond once an S1 incident is logged through one of the agreed channels.	**Service Level Type:** CSL **Frequency:** Monthly	>99% within 5 minutes	0
				>=97% and <99% within 5 minutes	5
				<97% within 5 minutes	6

#	Category/ Component	Definition	Information	Service Level value	Severity Level
6	Response time for a Severity 2 (S2) incident	Average Time is taken to acknowledge and respond once an S2 incident is logged through one of the agreed channels.	**Service Level Type:** CSL **Frequency:** Monthly	>98% within 10 minutes	0
				>=95% and <98% within 10 minutes	4
				<98% within 10 minutes	5
7	Response time for a Severity 3 (S3) incident	Average Time is taken to acknowledge and respond once an S2 ticket/incident is logged through one of the agreed channels	**Service Level Type:** CSL **Frequency:** Monthly	>90% within 15 minutes	0
				>=80% and <90% within 15 minutes	3
				<90% within 15 minutes	4
8	Resolution time for an S1 incident	Time taken to resolve the reported problem	**Service Level Type:** CSL **Frequency:** Monthly	>99% within 120 minutes	0
				>=97% and <99% within 120 minutes	6
				<97% within 120 minutes	7
9	Resolution time for an S2 incident	Time is taken to resolve the reported problem.	**Service Level Type:** CSL **Frequency:** Monthly	>99% within 6 hours	0
				>=97% and <99% within 6 hours	5
				<97% within 6 hours	6
10	Resolution time for an S3 incident	Time is taken to resolve the reported problem	**Service Level Type:** CSL	>99% within 16 hours	0
				>=97% and <99% within 16 hours	4

#	Category/ Component	Definition	Information	Service Level value	Severity Level
			Frequency: Monthly	<97% within 16 hours	5
11	Root cause analysis completed for S1 Incidents	RCA report submission timeline	**Service Level Type:** KPI **Frequency:** Monthly	>=95% within 24 hours	N/A
12	Open Incidents over 30 days	% of Incidents opened over 30 days from the date of origin	**Service Level Type:** KPI **Frequency:** Monthly	<=2%	N/A
13	Level of automation of incident capture	Critical incidents (S1/S2) raised automatically vs. by user	**Service Level Type:** KPI **Frequency:** Monthly	>=90%	N/A
14	Incident Quality	Percentage of times the correct KB article is attached to the Resolved incident	**Service Level Type:** KPI **Frequency:** Monthly	>=95%	N/A

Change management SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1	Completion Time of Emergency CRs	% of Emergency Change Requests completed within time period defined by GeM	**Service Level Type:** CSL **Frequency:** Monthly	>=99%	0
				>=95% and <99%	4
				<95%	6
2	Completion Time of Non-Emergency CRs	% of other CRs (all CRs excluding Emergency CRs) completed within time period mutually defined by MSP and GeM	**Service Level Type:** CSL **Frequency:** Monthly	>=99%	0
				>=95% and <99%	3
				<95%	5
3	Compliance to Change Control Procedures	100% of changes should follow & comply to formal change control procedures	**Service Level Type:** CSL **Frequency:** Monthly	100% of changes should follow formal change control procedures.	0.01% of the Quarterly Payment shall be levied as Liquidated Damages for every non-compliance.
4				>=99%	0

#	Category/ Component	Definition	Information	Service Level value	Severity Level
	Timely completion of O&M related changes	% of O&M changes completed within time period defined by GeM	**Service Level Type:** CSL **Frequency:** Monthly	>=95% and <99%	4
				<95%	6

Project Management SLAs

#	Category/Component	Definition	Information	Service Level value	Security Level
1	Project Management - Schedule Variance	**Metric:** % Variance between allotted time for development / change and estimated time **Formula:** Schedule Variance = (Actual Elapsed Time – Estimated Elapsed Time) / Estimated Elapsed Time	**Service Level Type:** CSL **Frequency:** Quarterly	<=5%	0
				>5%	4

#	Category/Component	Definition	Information	Service Level value	Security Level
2	Application Development and Maintenance	**Metric:** Compliance to CMMI Level 5 by the MSP in the area of Application Development and Maintenance	**Service Level Type:** CSL	Level 5 Assessment / Certificate in place (100%)	0
				Level 5 Assessment / Certificate lapsed (< 100%)	5
3	Availability of MSP Named Resources	**Metric:** Number of Manpower days for specified named resources by MSP. **Measurement:** Availability = (Round (GeM working day for 20 individuals * 0.85) - Exceptions/allowed absences) **Total LD** = SUM of LDs for each roles ((Expected Present - Actual Present) * LD Amount for the role)	**Service Level Type:** CSL **Frequency:** Monthly	99%	0
				>=97% to <99%	6
				>=95% to <97%	7
				<95%	8
				<100% adherence	3
4	Reporting - Monitoring of System	Availability of a dashboard to track and monitor 100% of the SLAs and KPIs	**Service Level Type:** CSL	100%	0

#	Category/Component	Definition	Information	Service Level value	Security Level
		How: Availability of dashboard and generation of reports in prescribed format **Period of Measurement:** Business hours (9 am to 7 pm)	**Frequency:** Quarterly	<100%	3

Business Services SLAs

#	Category/Component	Definition	Information	Service Level value	Severity Level
1	Buyer Registration	Registration process completion time as the difference between user creation request received from front end at click of Submit button and processing the data at server end and sending response back to the front end For delay of each additional 1 day after 7 days, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages	**Service Level Type:** CSL **Frequency:** Monthly	< = 7 days	0
				> 7 days	5
2	Seller Registration	Registration process completion time as the difference between user creation request	**Service Level Type:** CSL	< = 2 days	0

#	Category/Component	Definition	Information	Service Level value	Severity Level
		received from front end at click of Submit button and processing the data at server end and sending response back to the front end. For delay of each additional 1 day after 7 days, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages	**Frequency:** Monthly	> 2 and < = 4 days	3
				> 4 and < = 7 days	4
				> 7 days	5
3	Marketing & Promotions Activities	MSP to take approval from GeM officials and perform the approved activities as per approved timelines. For delay of each additional week or part thereof after 17 days, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages	**Service Level Type:** CSL **Frequency:** Monthly	< 7 days	0
				> 7 days & <= 10 days	4
				> 10 days & <= 15 days	5
				> 15 days & <= 17 days	6

8.6.9.2   Service Level Measurement and Common Definitions

1. The calculation of the MSP's performance against the following Service Levels shall be adjusted to remove the impact of the following events (should they arise):

   a. any security issues caused by pre-existing published exploitable vulnerabilities (remediation of pre-existing vulnerabilities can be requested via agreed Change control);

   b. or unplanned changes to the In-Scope Systems by GeM or any GeM third party;

   c. any impact on MSP services caused due to the network services, network outage (s), network latency or network performance issues;

   d. any documented and jointly agreed on the risk that requires remediation but where the GeM agrees that no remediation is required;

2. For Service Levels where any action is required by GeM or any of GeM's third parties, the calculation of such Service Level shall cease at the time MSP requests such action from the GeM or the relevant third party and the calculation of such Service Level shall commence at the time the relevant action is completed by GeM or the relevant third party.

3. The following tables set out the definitions and calculation methodologies for the Service Levels set out in this Appendix.

Description	Measurement Definition and Formula
Response time for an S1 incident	**Definition:** Time to acknowledge that a Severity 1 Incident has occurred. The response time begins when a Severity 1 Incident is logged into ITSM or from an auto-generated Incident. The clock on S1 incidents applies on 24 hours x 7 days a week basis. **Calculation formula:** (Number of Severity 1 Incidents assigned to MSP for which the Response Time for such Priority Level were met) / (Total Number of Severity 1 Incidents assigned to MSP) * 100 **Data Source:** ITSM

Description	Measurement Definition and Formula
Response time for an S2 incident	**Definition:** Time to acknowledge that a Severity 2 Incident has occurred. The response time begins when a Severity 2 Incident is logged into ITSM or from an auto-generated Incident. The clock on S2 incidents applies on 24 hours x 7 days a week basis. **Calculation formula:** (Number of Severity 2 Incidents assigned to MSP for which the Response Time for such Priority Level were met) / (Total Number of Severity 2 Incidents assigned to MSP) * 100 **Data Source:** ITSM
Response time for an S3 incident	**Definition:** Time to acknowledge that a Severity 3 Incident has occurred. The response time begins when a Severity 3 Incident is logged into ITSM or from an auto-generated Incident. The clock on S3 incidents applies in business hours of the geography from the incident is raised i.e., between 9 am and 6 pm. **Calculation formula:** (Number of Severity 3 Incidents assigned to MSP for which the Response Time for such Priority Level were met) / (Total Number of Severity 3 Incidents assigned to MSP) * 100 **Data Source:** ITSM
Resolution time for an S1 incident	**Definition:** The Resolution time starts from the time the Severity 1 Incident is assigned by MSP to MSP's support team queue in the ITSM during the hours of coverage, or (in respect of a Severity 1 Incidents via on-call Support outside of the Hours of Coverage) when the Severity 1 Incident is first notified to a member of MSP's support team nominated to receive requests for on-call support. The clock on S1 incidents applies on 24 hours x 7 days a week basis. The Resolution time will end when the ITSM is updated by MSP's support team to reflect that the Severity 1 Incident has been Resolved having followed the Incident Management process agreed by the Parties during the implementation of Services. The Resolution time shall not include the time between the Severity 1 Incident being Resolved and the GeM confirming that the Resolution is accepted (or that the Resolution is not accepted) but will include the time incurred by MSP in undertaking any further remedial work.

Description	Measurement Definition and Formula
	Calculation formula: (Number of Severity 1 Incidents assigned to MSP for which the Resolution Time for such Priority Level were met) / (Total Number of Severity 1 Incidents assigned to MSP) * 100 **Data Source:** ITSM
Resolution time for an S2 incident	**Definition:** The Resolution time starts from the time the Severity 2 Incident is assigned by MSP to MSP's support team queue in the ITSM during the Hours of Coverage or (in respect of a Severity 2 Incidents via on-call Support outside of the Hours of Coverage). The clock on S2 incidents applies on 24 hours x 7 days a week basis. The Resolution time will end when the ITSM is updated by MSP's support team to reflect that the Severity 2 Incident has been Resolved having followed the Incident Management process agreed by the Parties during the implementation of Services. The Resolution time shall not include the time between the Severity 2 Incident being Resolved and the GeM confirming that the Resolution is accepted (or that the Resolution is not accepted) but will include the time incurred by MSP in undertaking any further remedial work. **Calculation formula:** (Number of Severity 2 Incidents assigned to MSP for which the Resolution Time for such Priority Level were met) / (Total Number of Severity 2 Incidents assigned to MSP) * 100 **Data Source:** ITSM
Resolution time for an S3 incident	**Definition:** The Resolution time starts from the time the Severity 2 Incident is assigned by MSP to MSP's support team queue in the ITSM during the Hours of Coverage. The clock on S3 incidents applies in business hours of the geography from the incident is raised i.e., between 9 am and 6 pm The Resolution time will end when the ITSM is updated by MSP's support team to reflect that the Severity 3 Incident has been Resolved having followed the Incident Management process agreed by the Parties during the implementation of Services. The Resolution time shall not include the time between the Severity 3 Incident being Resolved and the GeM confirming that the Resolution is

Description	Measurement Definition and Formula
	accepted (or that the Resolution is not accepted) but will include the time incurred by MSP in undertaking any further remedial work. **Calculation formula:** (Number of Severity 3 Incidents assigned to MSP for which the Resolution Time for such Priority Level were met) / (Total Number of Severity 3 Incidents assigned to MSP) * 100 **Data Source:** ITSM
Root cause analysis completed for S1 Incidents	**Definition:** Root cause analysis completed for S1 Incidents is defined as the percentage of root cause analysis completed for S1 Incidents within the defined measure. The measure would start from the time problem record for closed S1 incident is created in the ITSM system. **Calculation formula:** (Total number of S1 incidents assigned to MSP where RCA was provided within defined measure / Total number of S1 incidents assigned to MSP for RCA) * 100 **Data Source:** ITSM System
Reopened Incidents	**Definition:** Reopened incidents are defined as the incidents which are re-opened after they were set to Resolved status. **Calculation formula:** (Total number of reopened incidents assigned to MSP / Total number of incidents assigned to MSP) * 100 **Data Source:** ITSM System
Open Incidents over 30 days	**Definition:** Open incidents are the incidents that are currently Open and not set to Resolved or Closed status. **Calculation formula:** (Number of Incidents assigned to MSP open over 30 days / Total Number of Incidents assigned to MSP) * 100 **Data Source:** ITSM System
Incident Quality	**Definition:** Incident Quality is defined as the Incidents set to Resolved or Closed status and the correct KB article is referenced in the Incident record. **Calculation formula:** (Number of Incidents Resolved or Closed by MSP using correct KB Article / Total Number of Incidents Resolved or Closed by MSP where KB Article is attached) * 100

Description	Measurement Definition and Formula
	Data Source: ITSM
Level of automation of incident capture	**Definition:** Level of automation of incident capture is defined as the Severity 1 and 2 Critical incidents logged via the tool. **Calculation formula:** (Total number of S1/S2 Critical Incidents logged via tool / Total number of S1/S2 Critical Incidents logged) * 100 **Data Source:** ITSM

Table 114: Service Level Definitions and Calculation methodologies Part 1

Description	Measurement Definition and Formula
Service Management (SIAM) - On-Time Delivery of Service Management (SIAM) Reports	**Definition:** On-time Delivery of Service Management (SIAM) Reports are the agreed monthly Service Management (SIAM) reports delivered to the GeM - by the 10th calendar day of the month following the reporting period. **Calculation formula:** (Number of agreed monthly Service Management (SIAM) reports that were delivered to GeM by 10th calendar day of the month following the reporting period) / (Total number of agreed monthly Service Management (SIAM) reports that were due during the reporting period) * 100 **Data source:** To be agreed (e.g., SharePoint timestamp)
Service Management (SIAM) - Time is taken to open a Major Incident bridge	**Definition:** Time taken to open Major Incident bridge is the time in which the Major Incident bridge invite is sent out to an agreed distribution list from the time Service Management (SIAM) team was notified about the Major Incident **Calculation formula:** (Number of Major Incidents during the reporting period where the major incident bridge was <= 15 minutes from the time Service Management (SIAM) team was notified about the major incident) / (Total number of Major Incidents during the reporting period) * 100 **Data source:** Major Incident whiteboard
Service Management (SIAM) - On-time occurrence of Major Incident	**Definition:** On-time occurrence of Major Incident Review of S1 incidents is where Major Incident Review is set up within 2 Business Days after the S1 Incident is resolved. **Calculation formula:** (Number of S1 Incidents during the reporting period where Major Incident Review is set-up within 2 Business Days after the S1 Incident is resolved) / (Total number of S1 Incidents resolved during the reporting period) * 100

Review of S1 incidents	**Data source:** Outlook meeting time stamp
Service Management (SIAM) - On-time occurrence of Post Implementation Review for failed Changes	**Definition:** On-time occurrence of Post Implementation Review for failed Changes is where Post Implementation Review is set-up within 2 Business Days from the identification of the Failed Change **Calculation formula:** (Number of identified Failed Changes during the reporting period where Post Implementation Review was set-up within 2 Business Days from the identification of the Failed Change) / (Total number of identified Failed Changes during the reporting period) * 100 **Data source:** Outlook meeting time stamp

Table 115: Service Level Definitions and Calculation methodologies Part 2

8.6.9.3 Priority Level Definition and Priority Matrix

8.6.9.3.1 Priority Level Definitions

Priority Level	Definitions	Examples
Severity Level 1 — Emergency/Urgent Critical Business Impact	The Incident has caused a complete and immediate work stoppage affecting primary business processes, broad group of users on GeM, service, traffic, billing and maintenance capabilities on GeM. Critical problems resulting in a stoppage of revenue generation or commercial process fulfilment and require immediate	Business and Financial Examples 1. Enterprise-wide visibility. 2. Catastrophic impact. 3. Critical to major impact on business revenue. 4. Buyers/Sellers are unable to process any business transactions. 5. The failure creates serious business and financial exposure. System / Infrastructure Examples 1. Multiple Systems and/or functions are down. 2. Multiple locations, buildings, departments. 3. Network outage: LAN/WAN/Internet failure. 4. Security threat, i.e., virus or worm spread through the enterprise. 5. Long-term impact on the operations of the majority of the entire enterprise.

Priority Level	Definitions	Examples
	corrective action, regardless of time of the day or day of the week.	6. System or certain functions/services are down. 7. The failure causes a system to be inoperable to all users, total loss of functionality. 8. Many or major files lost, large data corruption. 9. A system or Network that is chronically out of service or continues to fail repeatedly. 10. Critical business cycles (e.g., month/quarterly/year-end financial activity). 11. Critical business processes (e.g., payment runs, batch jobs). 12. A whole division, multiple workgroups or departments. 13. Affects a large part of Buyers, a whole department. 14. > 80% of department, office, site or user-base affected.
Severity Level 2 — High **Major Business Impact**	The Incident has affected a business process in such a way that business functions are severely degraded, or multiple users are affected, or affecting system operation, maintenance and administration, etc. The urgency is less than in critical situations because of a less immediate or impending effect on system performance,	Business & Financial 1. Medium visibility and moderate impact on revenue. 2. The significant impact may threaten future productivity if the issue is not resolved. System / Infrastructure 1. System usage is limited. 2. Slow proposal (network or application) and loss of functionality. 3. Few files were lost or corrupted. GeM- Impact 1. Buyers / Sellers were unable to perform some portion of their job function. 2. > 50% of department, office, site or user-base affected

Priority Level	Definitions	Examples
	customers or revenue.	
Severity Level 3 — Medium Moderate Business Impact	The Incident has affected a business process in such a way that certain functions are unavailable to End Users or a system or service is degraded. Minor problems that do not significantly impair the functions of the system and do not seriously affect service to the customer.	Business & Financial 1. Minimal immediate business or financial exposure. System / Infrastructure 1. Functionality is degraded but can be circumvented. GeM- Impact 1. Buyer / Seller was unable to perform a minor portion of their job. 2. No business or financial impact. 3. Scheduled or planned work and coordinated with GeM. 4. >10% of department, office, site or user-base impacted.

Table 116: Priority level definitions

8.6.9.3.2   Priority Level Matrix

Indicative Priority Level is defined as the intersection of the applicable Urgency and Impact in the ITSM tool.

PRIORITY MATRIX		1 – Extensive / Widespread	2 – Significant / Large	3 – Moderate / Limited
URGENCY	1 – Critical	Severity 1	Severity 1	Severity 2
	2 – High	Severity 1	Severity 2	Severity 2
	3 – Medium	Severity 2	Severity 3	Severity 3
	4 – Low	Severity 3	Severity 3	Severity 3

Table 117: Priority level matrix

8.6.10 APPENDIX II: Existing SLAs applicable on current GeM platform

8.6.10.1.1 System Availability SLAs

#	Category/ Component	Definition	Information	Service Level value	Severity Level
1.	Availability of GeM Web Portal	% of Uptime for GEM Web Portal Metric: % of Uptime for GEM Web Portal Formula: Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 GEM web portal is expected to be available 24 x 7. Total Downtime - Total cumulative time the GEM Web portal is NOT available. Planned Downtime - Total maintenance time as defined and agreed upon by MSP and the Purchaser. Total Time - 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages	**Frequency:** Monthly	>=99.9%	0
				<99.99% and >= 99.5%	4
				<99.5% and >= 99.0%	5
				<99.0% and >= 98.5%	6
				<98.5% and >= 98.0%	7
				<98.0%	8

#	Category/ Component	Definition	Information	Service Level value	Severity Level
2	Availability of the below mentioned five (05) critical Services & Functionalities of the GeM System: 1.E-Tendering(Bid/RA-Reverse Auction) 2. Forward Auction 3. Plain buy / L1 Buy 4. Buyer Registration 5. SSO/ARX * The Purchaser reserves the right to change the above services & functionalities as per business requirements	The availability of the mentioned five (05) critical Services & Functionalities of the GeM System measured as % uptime Metric: % of Uptime Formula: Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 GEM Services – All Modules are expected to be available 24 x 7. Total Downtime – Total cumulative time the mentioned GEM Services & Functionalities are NOT Available. Planned Downtime -Total maintenance time as defined and agreed upon by MSP and the Purchaser. Total Time - 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages.	**Frequency:** Monthly	>=99.9%	0
				<99.9% and >= 99.5%	4
				<99.5% and >= 99.0%	5
				<99.0% and >= 98.5%	6
				<98.5% and >= 98.0%	7
				<98.0%	8
3	Availability of other critical Services such as 1. Seller Registration, 2. Training Module,	The availability of the mentioned 10 Services & Functionalities of the GeM System measured as % uptime Metric: % of Uptime Formula: Uptime % = {1-	**Frequency:** Monthly	>=99.9%	0
				<99.9% and >= 99.5%	1
				<99.5% and >= 99.0%	2

#	Category/ Component	Definition	Information	Service Level value	Severity Level
	3. Reporting & Analytics 4. Assets BG 5. Assets MKP 6. Fulfillment 7. CMS 8. Payments 9. Seller catalog admin 10. Buyer Order Acceptance	[(Total Downtime) / (Total Time – Planned Downtime)]} *100 GEM Services – All Modules are expected to be available 24 x 7. Total Downtime - Total cumulative time the mentioned GEM Services & Functionalities are NOT Available. Planned Downtime -Total maintenance time as defined and agreed upon by MSP and the Purchaser. Total Time - 24 X 7 measured over a period of month. For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages		<99.0% and >= 98.5%	3
				<98.5% and >= 98.0%	4
				<98.0%	5
4	Availability of Bandwidth (Internet and WAN MPLS)	GeM System Availability over MPLS/ Internet For each additional drop of 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages. Name of Artifact: Link Availability Report (Month)	**Frequency**: Monthly	>= 99.9%	0
				<99.9% and >= 99.5%	1
				<99.5% and >= 99.0%	2
				<99.0% and >= 98.5%	3
				<98.5% and >= 98.0%	4
				<98.0%	5

8.6.10.1.2 Cloud Service SLAs

#	Category/Component	Definition	Information	Service Level value	Security Level
1	RTO	Based on the successful operations from DR Site and restoring the services back For delay of each additional 2 Hours or part thereof after 6 Hours, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated	**Frequency**: Half Yearly (as per DC-DR Drill)	< 2 Hours	0
				2-4 Hours	5
				4-6 Hours	7
				>6 Hours	8
2	RPO	Based on the successful operations from DR Site and restoring the services back. For delay of each additional 30 minutes or part thereof after 90 minutes, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages.	**Frequency:** Half Yearly (as per DC-DR Drill)	< 30 Mins	0
				30-60 Mins	5
				60-90 Mins	7
				> 90 Mins	8

#	Category/Component	Definition	Information	Service Level value	Security Level
3	Provisioning and deprovisioning of Virtual Machines	Per Occurrence. This will be calculated monthly. For delay of each additional 30 minutes or part thereof after 45 minutes, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages.	**Frequency:** Monthly	<15 Mins	0
				15-45 Mins	6
4	DC-DR Drill	Number of Drills as per the defined Policy or at least 2 DR Drills in a year (once every 6 months) This will be measured every 6 months and the Liquidated Damages will be levied in the quarter following the end of the six month period.	**Frequency:** Half Yearly (as per DC-DR Drill)	0 Drill	0
				1 Drill	5
				2 Drills	6
5	Adherence to Backup Policy	Based on the backup policy of the Purchaser Target : · 100% backups taken on time as per the Purchaser' s Backup Policy 100% backups shipped to offsite location on schedule in accordance to the Purchaser' s Backup Policy 100% backup restoration testing on time in	**Frequency**: Monthly	100% backup on time as per backup policy	0
				< 100% backup restoration testing on time in accordance to the Purchaser's Backup Policy	3
				< 100% backups shipped to offsite location on schedule in accordance to the	4

#	Category/Component	Definition	Information	Service Level value	Security Level
		accordance to the Purchaser's Backup Policy		Purchaser's Backup Policy	
				< 100% backups taken on time as per the Purchaser's Backup Policy	5

8.6.10.1.3 Performance SLAs

#	Category/Component	Definition	Information	Service Level value	Security Level
1	Average page loading time for all services	Page loading time measured monthly. The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR	**Frequency:** Monthly	95% within the limit of 2 seconds	0
				Less than 95% Outside the limit of 2 seconds	2
2	Transaction response time except the transactions mentioned below in #3	Response time of services measured monthly The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR	**Frequency:** Monthly	95% within the limit of 2 seconds	0
				Less than 95% Outside the limit of 2 seconds	2

#	Category/Component	Definition	Information	Service Level value	Security Level
3	Transaction response time involving uploading/ downloading of documents (avg. size 2 MB)	Response time of services measured monthly The response will be measured from 10 desktops from GeM HQ at any given point in time for both DC & DR.	**Frequency:** Monthly	95% within the limit of 5 seconds	0
				Less than 95% Outside the limit of 2 seconds	2

8.6.10.1.4 Reporting SLAs

#	Category/Component	Definition	Information	Service Level value	Security Level
1	Reporting - Schedule Reporting	100% adherence to timelines specified in RFP	**Frequency:** Monthly	100% adherence	0
				< 100% adherence	3

8.7 Annexure G – Change Control Procedure

8.7.1 Purpose and Objective

1. The purpose of the Change Control procedure is to control changes in the GeM System environment throughout the tenure of the Agreement. The document also details the Change Request process to be followed in GeM whenever required.

2. The Change Control procedure has the following objectives:

   a. To protect the GeM System environment from uncontrolled changes.

   b. To minimize the occurrence of unintended effects during the implementation of necessary changes.

   c. To avoid implementation of any changes which is not reviewed, approved, or analyzed.

   d. To control the impact of changes and minimize the effect on effective as well as efficient service delivery.

   e. Help address issues pertaining to:

      i. What is considered a change request?

      ii. Need for a change request – business case / justification

      iii. What is the nature / type of change request?

      iv. What is the possible impact due to change request?

      v. What is the effort estimation to execute the change request?

      vi. Whether there is a requirement for additional payment to the MSP for the change?

8.7.2   What constitutes a Change Request?

Scope	Any internal stakeholder nominated by GeM (Originator) can submit the following types of issues to the change control system: 1. requests for requirements changes (additions, deletions, modifications) to the Scope of work (including software) 2. requests for enhancements in current production systems with functional requirements beyond the scope of this RFP and as defined during the business signoffs by the MSP, e.g., additional process steps to be introduced in a currently defined process flow This change control process applies to baseline work products created or managed by the members of GeM project, including but not limited to: 1. software that has been released to production 2. requirements specifications for GeM project 3. group procedures and processes 4. user roles and technical documentation Baseline work products are work products which have been formally reviewed and approved by GeM and deviations/changes to the same can only be made via formal change control procedure – SRS document acts as a baselined work product w.r.t system design. Interim or temporary work products created during the course of the project are not considered as baseline work products. Change control procedure shall be applicable to changes being requested after the completion of the Go-Live of the new platform as mentioned in the Implementation Schedule in Volume 1 Section 5 of this RFP. The following categories of changes (indicative) shall not be considered as a change request and shall be exempted from the Change Control Procedure:

Role	Description
	1. Any work arising in order to fix root causes behind Critical Service Levels or KPI defaults, as mentioned in Volume 1 Section 8.6 of this RFP – any software or hardware related changes for these should be done as per normal troubleshooting scope under O&M by MSP (e.g., any changes required to maintain the uptime of the portal as defined in SLA) 2. Any software changes required due to problems/bugs in the developed software/ application/ hardware will not be considered as part of change control and will have to be completed by the MSP at no additional cost (even if it requires any enhancements/ customizations) (e.g., changes required to fix abnormal functioning of modules such as Reverse Auction due to software bugs) 3. Any activity pertaining to day-to- day operations & maintenance of GeM platform and services such as uploading of a policy/ circular/ other documents on GeM platform, masking of company name on the marketplace, label changes, external firewall upgrade implementation of changes as per latest revenue policy such as re-configuring transaction charge limits & rules, etc. 4. Any changes undertaken by MSP on its own to improve processes and applications (e.g., any changes undertaken for simplification of business processes under MSP) 5. Any request pertaining to data assistance, system access, server access, etc. by GeM or any nominated authority on behalf of GeM from MSP, which doesn't require any modifications in the portal or back-end systems

8.7.3 Institutional Framework for Change Requests

Given below is the overall Institutional Framework required to be set up for the project:

Role	Description
Change Advisory Board (CAB) Chairperson	1. Nominated by GeM Board of Directors

Change Advisory Board	1. Members of Change Advisory Board (CAB) (indicative)
	    a. CAB Chairman
	    b. Nominee 1 (Member as nominated by GeM CEO- can be internal/ external stakeholder)

	c. Nominee 2 (Member as nominated by GeM CEO- can be internal/ external stakeholder)
	d. Chief Technology Officer, GeM
	e. Project Director, MSP
	f. GeM Nominee from Financial vertical
	6. Authorized to evaluate final effort estimates and cost sheets submitted by MSP in CR Form-3 and recommendations from CTO/ nominated authority (internal/ external) by GeM CEO/ CTO on CR Form-2, and give approval for the same
	7. Authorized to review, approve, and schedule all changes to the computing environment including software
	8. Authorized to review and support in handling escalations w.r.t CR Form-1, if required by Chief Marketplace Officer -Product/ Chief Marketplace Officer- Services/ any other nominated authority by GeM CEO/ GeM CEO
	9. CAB decision to be considered final and binding on all parties involved
	10. In case CAB does not reach an agreement, final decision-making authority is the chairperson of CAB and his decision in this case would be considered as final and binding
Change Request Management Committee (CRMC)	Members of Change Request Management Committee (CRMC) - 1. Chairperson of CRMC (Nominated by GeM CEO) 2. Nominee 1 (Member as nominated by GeM CEO - can be internal/ external stakeholder) 3. GeM Nominee 1 (Member as nominated by GeM CEO) 4. GeM Nominee 2 (Member as nominated by GeM CEO) 5. MSP Representative CRMC to evaluate CR Form-1 for in principal acceptance of "Change from Scope of work as per RFP" along with demarcation whether it is "Revenue Generating Change Request" or "Non-Revenue Generating Change Request", as defined below: 1. **Revenue generating change request:** Any change which results in incremental revenue for GeM as well as MSP from either the GeM platform or new offerings / functionalities / features enabled for GeM customers will be considered as a revenue generating change request. No payment would be made to MSP for development and deployment of such requests.

	2. **Non-revenue generating change request:** Any other change request, that does not qualify as a revenue generating change request, will be classified as a non-revenue generating change request. For example, development of Push button procurement functionality on GeM will be a revenue generating change request, whereas any process related to change in the Customer Service process will be a non-revenue generating change request.
Change request application	The Originator submits a valid issue or change requirement with all necessary information on the Change Management Tool, referred to as Change Request Application.
Change request	Once the reviewer approves the change request application submitted by the originator on whether it should be implemented or not, it would be regarded as a change request.
Originator	Any nominated person from GeM (basis role assigned) can be designated as originator by GeM. Originator shall submit a change request application, whenever required, via the change management portal. There can be multiple originators.
Reviewer	Any nominated person(s) from GeM (basis role assigned) who is responsible for the approval of change request application submitted by the originator on whether it should be implemented or not. There can be multiple reviewers.
Modifier	The person from the MSP team who is assigned responsibility for making changes in a work product in response to an approved change request; Modifier shall deploy the change and update the status of the request over time
Verifier	The person from GeM team who determines whether a change was made correctly. This can be an individual, group or a committee as required which will be nominated by the reviewer who approves the change request application. Upon successful verification of deployment of the change the status changes to "Verified". In case further modifications are required, the status changes to "Verified and resent for modification" on the tool. In certain cases, the verifier may be the same as originator, in which case, originator shall inspect and verify the change deployed. In case of originator being separate from the verifier, approvals of both

	originator and verifier would be required for confirmation of change request as verified.

Common communication process for Change Requests

Change Request Status	
Change Management Tool	MSP shall create a tool to digitize the Change Request process detailed below, and for tracking the status of all the Changes to be made (irrespective of whether it has been approved as a change request or not by CRMC). The tool shall allow filling and submission of different Change Request forms to be submitted (as described in Volume 1 Section 8.7.7 of this RFP) and shall capture details of all changes submitted, whether it was deemed a change request or no, category of change, change severity, timeline, status, etc. The tool should be integrated with GeM and MSP's Invoice and Payment management module and Project Management Tool. The tool should be configured such that artefacts/documents can also be uploaded on it. The tool should allocate a unique number to each change request application.
Status Changes	A requested change will pass through several possible statuses during its lifecycle. These statuses, and the criteria for moving from one status to another, are depicted below.
Notifications	Any time an issue status is changed, the change management tool will send an e-mail notification automatically to the change Originator, the change Modifier, and/or other relevant users within GeM (such as the Verifier), as specified below.

Change Request Application Status Flag: Corresponding to each unique change request application, this displays the Status of the change request application proposed

1. **Submitted:** The Originator has submitted a new change request application to the change management tool.

2. **Approved:** The change request application is approved by reviewer for implementation on the change management tool.

3. **Rejected:** The change request application is rejected by reviewer for implementation on the change management tool.

Change Request Approval Status Flag:- After decision by CRMC and escalations displays whether CR Form-1 pertaining to a change request application has been approved in principle or not

1. **CR Form-1 submitted:** MSP has submitted CR Form-1 on the change management tool

2. **Approved (Revenue Generating)/ Approved (Non-revenue Generating)/ Rejected:** CRMC, or authority reviewing escalation if any, has approved/ rejected CR Form-1 within principal acceptance/ rejection of "Change from Scope of work as per RFP" with demarcation whether it is "Revenue Generating Change Request" or "Non-Revenue Generating Change Request"

3. **CR Form-1 escalated:** MSP has raised escalations for CR Form-1 to Chief Marketplace Officer -Product/ Chief Marketplace Officer- Services/ any other nominated authority by GeM CEO or a second escalation to GeM CEO

Deliverables and Cost Approval Status Flag: This shows the status for deliverables and timelines approval process in case of Revenue Generating Request, and deliverables, timelines, and effort and cost estimates in case of Non-revenue Generating Request

1. **CR Form-2 submitted:** MSP has submitted CR Form-2 (with duly filled details around impact, deliverables, timelines, effort and cost estimates, as applicable in case of Revenue and Non-Revenue Generating Request) on the change management tool

2. **CR Form-2 approved/ rejected:** CTO/ nominated authority by GeM (internal/ external) has evaluated and approved/ rejected CR Form-2 on a preliminary basis

3. **CR Form-3 submitted:** MSP has submitted CR Form-3 on the tool (with actual effort and cost estimates and resources related undertaking updated, as applicable in case of Revenue and Non-Revenue Generating Request) on the change management tool for approval of CAB

4. **CR Form-3 approved/ rejected:** CAB, or CEO post escalation, has evaluated and approved/ rejected CR Form-3 detailing the final effort and cost estimates post development and deployment of change

5. **CR Form-3 escalated:** MSP has raised escalations for CR Form-3 to CEO

Change Request Implementation Status Flag: This shows the status of the implementation of the change request, such as:

1. **BRD Submitted**: MSP has submitted the final BRD on the change management tool.

2. **BRD approved:** Committee/ nominated authority by GeM CEO has reviewed and approved the BRD.

3. **Modified:** The Modifier has completed implementing the requested change.

4. **Verified:** The Verifier has confirmed that the modifications in affected work products were made correctly.

5. **Verified and resent for modification:** The Verifier notifies that the modifications in affected work products were not made correctly and requires more modifications.

6. **Cancelled:** The Originator or someone else decided to cancel/ discontinue an approved change.

7. **Deferred:** The Originator or someone else decided to defer an approved change.

8. **Invoice submitted:** MSP has submitted invoice on the payment management module of GeM

9. **Payment completed:** GeM Finance team has made payment on the base of verification of change status and Invoice raised by MSP

8.7.4   Change Control Process

1. The Originator (basis role assigned) submits a change request application i.e., valid issue or change requirement with all necessary information in Part A of CR Form-1 (as given in Volume 1 Section 8.1 of this RFP) on the Change Management tool.

2. Reviewer (basis role assigned) evaluates whether the change is to be implemented or not and approves/ rejects Change request application on the change management tool.

3. The MSP fills and submits Part B of CR Form-1 (as given in Volume 1 Section 8.7.7 of this RFP) on Change management tool to CRMC. This form includes details such as application modules impacted, databases impacted, infrastructures impacted, etc.

4. The MSP shall prepare Business Requirement Document (BRD) for the change request in parallel, without waiting for consideration with CRMC. If required, MSP nodal person can seek discussion with Originator or any other person within GeM for required detailing on the change request and submit the BRD for approval of committee or authority nominated by GeM CEO (in consultation with the Originator).

5. CR Form-1 shall be evaluated by Change Request Management Committee (CRMC) for in principal acceptance of "Change from Scope of work as per RFP" with demarcation whether it is "Revenue Generating Change Request" or "Non-Revenue Generating Change Request". In case it is a revenue generating request, no financial implication is to be considered.

6. MSP may accept the decision of CRMC or submit its representations to the Chief Marketplace Officer- Product/ Chief Marketplace Officer- Services/ any other nominated authority by GeM CEO. The authority may seek views of CRMC or any other committee/ officer and communicate its decision to MSP.

7. MSP may accept the decision of authority or in case of rare instances submit its representations to the CEO of GeM. CEO may seek views of authority giving the decision or any other committee / officer and communicate decision to MSP. CEO's decision in this case would be final and binding.

8. After approval of CR Form-1 and BRD, Part A of CR Form-2 is auto populated on the Change Management tool. MSP fills and submits Part B of CR Form-2 containing timelines, detailed effort estimates and cost sheets on the tool (effort and cost estimate section need not be filled in case of revenue generating change request; tool shall make the fields to be filled mandatory basis the type of change request - revenue generating or non-revenue generating) for approval of CTO/ other nominated authority by GeM CEO or CTO (can be internal or external)

9. CTO/ nominated authority by GeM CEO or CTO reviews CR Form-2 and takes a preliminary decision on cost estimates provided by the MSP and consequently provides a preliminary approval. MSP may be called upon by CTO/ nominated authority by GeM CEO or CTO to provide detailed presentation/ explanation to justify its cost estimates to ensure proper assessment and decision.

10. In case of Non-Emergency change request the development and deployment process will start after the preliminary approval of CR Form-2 by CTO/ nominated authority by GeM (depicted in Figure 69 below). MSP shall assign a 'Modifier' who shall be responsible to make changes in a work product in response to an approved change request. The Modifier and other resources working on implementation of a change request shall co-ordinate with Originator/ GeM nominated Point of Contacts regularly and report daily progress.

11. After the changes are made by modifier, he would change the status of the request as '**Modified**' on the tool. The Originator and Verifier will accordingly be notified.

12. The request would be verified by the verifier assigned by GeM. Verifier may be the originator himself.

13. Verifier reviews the work done by modifier. If verification is successful, the Verifier sets the status to **Verified**. The tool sends an e-mail to the Originator and Modifier. If verification is not successful, the Verifier shares relevant comments/ proposes further modifications in the 'Response' attribute and sets the status to **Verified and Resent for Modification**. In case of originator being separate from the verifier, approvals of both originator and verifier would be required for confirmation of change request as verified. The modifier makes the further modifications and updates the status accordingly.

14. For a problem report issue or an enhancement request issue, the Modifier installs the modified work product as appropriate and updates the product baseline. For requirements changes, the Modifier updates version numbers on all modified work products per the project's version control procedure, check them back into the version control system, updates requirements traceability information and requirements status attributes as necessary and updates the requirements baseline.

15. Verifier verifies the change made and sets the status to '**Verified**'. In case of originator being separate from the verifier, approvals of both originator and verifier would be required for confirmation of change request as verified.

16. Post verification of change request, MSP shall submit CR Form-3 (only in case of non-revenue generating change request) with details around resources deployed (name and designation), actual effort estimates and cost sheets, deliverables submitted along with an undertaking that the resources that developed and deployed the change request were separate from the resources that were deployed under the original Scope of Work as per this RFP.

17. CR Form-3 is presented to CAB for necessary approval / decision. MSP may be called upon by CAB to provide detailed presentation/ explanation to justify its cost estimates to ensure proper assessment and decision.

18. MSP shall, after receiving the approval of CAB, submit the invoice for a change request implemented on the Change Management tool (tool shall be linked with payment management modules between GeM and MSP). Post this the status changes to 'Invoice submitted'. The GeM Finance Team reviews the invoice, approved CR Form-3 available on the tool, and change request verification status and accordingly processes the payment to MSP. When payment is complete, the status on the tool changes to 'Payment Complete'. The tool should enable the MSP team to raise an invoice only when the cumulative man months

utilized on all the verified, non-revenue generating change requests have exceeded a total of 2,000 man months.

19. MSP may accept the decision of CAB or in case of rare instances submit its representations to GeM CEO. CEO may seek views of both CAB and MSP. CEO's decision in this case would be final and binding.

20. In case of "Emergency" category changes, after the Originator submits the change request application and it gets approved by the reviewer, the request could be marked as Emergency by the authorized individuals (GeM CEO/ nominated authority by GeM CEO). For all changes categorized and approved as 'Emergency' category change, the above process shall be bypassed.

21. For Emergency category changes, the process of development and deployment of required change shall start as soon as the BRD is approved (approval of any 1 relevant ACEO will be sufficient in case of 'Emergency' requests) and CR Form-1 and CR Form-2 and 3 shall be submitted/approved parallelly with development/deployment of the change request. The same has been depicted in Figure 70 below.
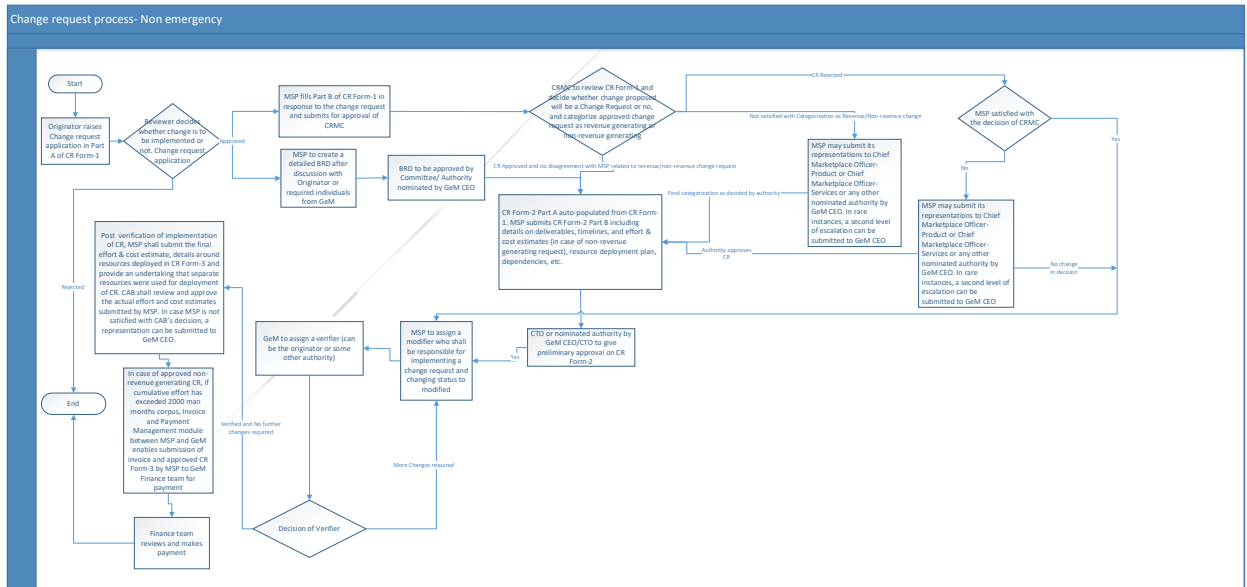
Figure 69: Change request process for Non-Emergency change request
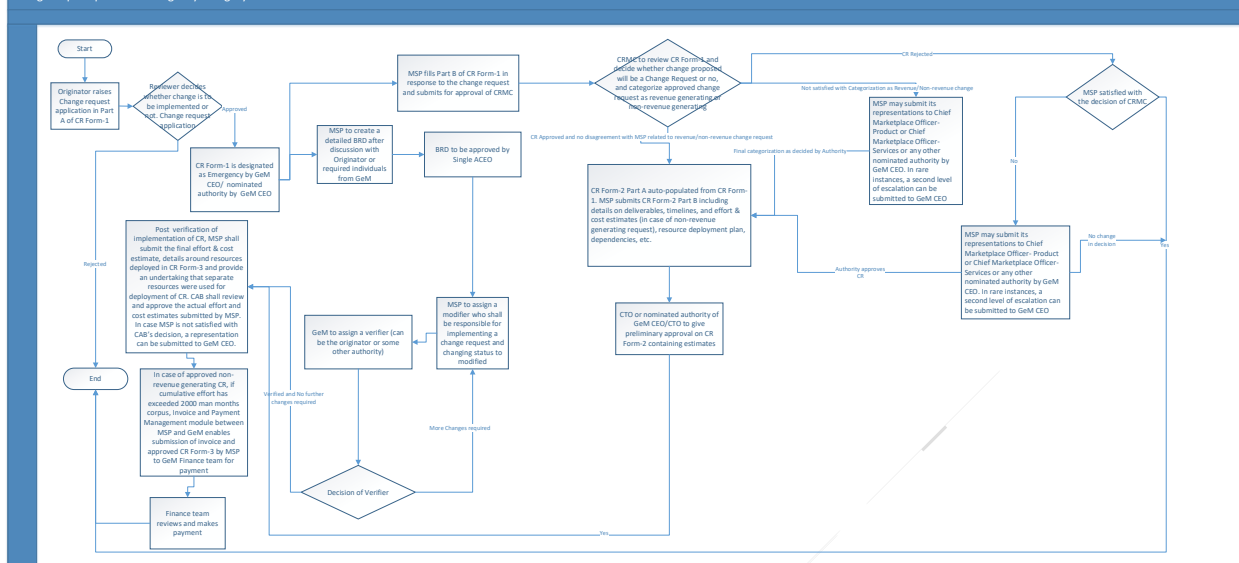
Figure 70: Change request process for Emergency change request

Note:

1. Indicative timelines need to be built in the system basis which notifications and reminders should also be raised. Timelines for each of the process steps are to be finalized by mutual agreement between GeM and MSP before the Go-live of the new GeM Platform.

S.No	Particulars	Timeline
1	CR Form-1 Submission by MSP	5 working days from the date Change request application is approved as change request
3	Escalation to Chief Marketplace Officer – Product/ Chief Marketplace Officer – Services/ Any other nominated authority by GeM CEO in case of disagreement in CR Form-1 with CRMC	5 working days from the response of CRMC
4	Chief Marketplace Officer – Product/ Chief Marketplace Officer – Services/ Any other	5 working days from submission of representations by MSP

	nominated authority by GeM CEO to resolve the disagreement	
5	Escalation to GeM CEO in case of rare instances of disagreement with Chief Marketplace Officer – Product/ Chief Marketplace Officer – Services/ Any other nominated authority by GeM CEO	5 working days from the response of Chief Marketplace Officer – Product/ Chief Marketplace Officer – Services/ Any other nominated authority by GeM CEO
6	CEO resolves the disagreement	5 working days from submission of representations by MSP
7	BRD submission for approval	As per timelines aligned for each BRD
8	Approval of BRD by committee/ authority nominated by GeM CEO	To be mutually agreed between GeM and MSP
9	CR Form-2 Submission by MSP for approval of CTO/ nominated authority by GeM CEO/ CTO	5 working days from approval/resolution of CR Form -1
9	Approval of CR Form -2 by CTO/ nominated authority by GeM CEO/ CTO	10 working days from submission of CR Form-2
10	Submission of actual efforts and cost sheets and resources related undertaking by MSP via CR Form-3	5 working days from successful deployment and verification of change requests

In case there is a need for GeM to discontinue a change pertaining to an approved change request during or after implementation, MSP shall be paid the amount basis closest milestone or effort estimate as per mutual agreement by GeM and MSP.

Change severity matrix

Severity	Examples
Emergency	Any change that is required to be made immediately, bypassing the change control process temporarily. (Example-implementing a critical security patch, the product does not function at all or crashes, the wrong results are generated, etc.). This severity category requires an approval from GeM CEO/ nominated authority by GeM CEO to be deemed as 'Emergency'.
Non-Emergency	**Non-Emergency Changes will be routed through the Change Control Procedure mentioned in this section for deployment.** (Example- cosmetic problems, usability improvements, unclear error messages, problem adversely affects product functioning or customer experience, but a workaround is available, new development required for enhanced customer experience/process efficiency, etc.)

8.7.5   Proposed Categories of Change

8.7.5.1   Application Software

1. Description

   Change Request for any new module/change in module/functionality/process re-engineering etc., any new services and any new forms, etc.

2. Documents Required

   a. Detailed Project Plan

   b. Effort Estimates (module wise/process-wise/screen wise, as applicable)

   c. Resource Deployment Plan/Types of Resources

   d. Resource Plotting Sheet

e.   CVs/Profiles of Resources (if required)

f.   Techno-Commercial Proposal

8.7.5.2   Infrastructure Procurement

1.   Description

Additional computing resources, bandwidth, as per GeM application scalability requirements.

2.   Documents Required

a.   Quantity (BoM)

b.   Specifications

c.   Software Licenses if any

d.   Warranty & Support Services details

e.   Efforts required, resource quantity and category

f.   Any other details as applicable

8.7.5.3   Helpdesk

1.   Description

Additional manpower/seating capacity, based on call volume

2.   Documents Required

a.   Call Volume analysis/report

b.   Resource Deployment Plan/Types of Resources

c.   CVs/Profiles of Resources (if required)

d.   Techno-Commercial Proposal

<u>Note:</u> The categories of change, and corresponding description and list of documents required mentioned above are only indicative and these may be changed as per directions from GeM.

8.7.6 Change Control Procedure General Guidelines

1. Parties, while evaluating and finalizing the Change Request, shall consider the change in the context of the following parameter, namely whether the change is beyond the Scope of Services including ancillary and concomitant services required and as detailed in the sign-off version of all required documents.

2. Implementation status of all approved Change requests will be reported quarterly to GeM who will review progress and prioritize as needed. The MSP shall be required to implement any proposed changes once approved with effect from the date agreed for implementation.

3. The MSP may also submit any queries/clarifications that it may have with respect to the implementation of the Change requested. If the MSP fails to implement any approved CR within the prescribed time duration, appropriate SLA and Liquidated Damages will be levied on the MSP. The MSP must not deny the implementation of any Change requested by CAB under any circumstances unless technical feasibility is in question. In all such matters, GeM's decision will be final and binding on all parties.

4. All forms shall be submitted with all required information duly filled by the MSP. If required, relevant authorities managing the Change Control Procedure (CRMC, CAB, CTO, other nominated authorities, etc.) may seek any additional information from the MSP at any stage of the process

5. The acceptance criteria for any such Change Request should be mentioned in the BRD prepared by MSP and mutually agreed between GeM and MSP.

6. The MSP must take all necessary steps to implement the Change as per the project plan submitted without compromising on quality and performance standards. If GeM alters the requirement in between or post approval of BRD & efforts of MSP, then such delay, MSP will not be held responsible. If the MSP fails to comply with the acceptable standards & requirements of implementing the Change requested or denies implementation of the Change requested at any stage during the Agreement period, CAB will have complete authority to get the Change implemented from any of the third-party/nominated government agency independently. In all such cases, the entire cost of Change implementation will be recovered completely from the MSP, along with applicable interest. Also, CAB reserves the right to impose any other kind of deductions depending upon the gravity of impact on the Service Delivery due to non-implementation of the Change requested. In all such matters, the decision of CAB will be final and binding on all parties.

7. If GeM provides additional changes/ new requirements for a change request under implementation, the changes will be considered a part of the same Change Request. MSP shall

update the BRD, and effort and cost estimates as per mutual agreement between GeM and MSP. The requirements for the required infrastructure to implement the change should be specified by the MSP so that CAB can make necessary provisions.

8. In case any deficiency is identified in a change request implemented by MSP at a later stage, MSP shall rectify the deficiencies without any additional change request and cost to GeM.

9. In case it is identified at a later stage that multiple change requests have been raised for the implementation of a particular change/ feature, GeM shall reserve the right to re-estimate costs and adjust any double payments made previously against the next quarterly payout to MSP.

10. A fixed blended rate of INR 2.5 Lakhs per man month shall be used to calculate cost pertaining to approved non-revenue change requests. An annual increase in price at a rate of 6% shall be allowed to account for inflation.

11. MSP will factor in 2000 man-months of efforts towards non-revenue generating change requests as part of this RFP. This corpus shall be used on a first-come-first-serve basis. Any effort beyond 2000 man-months will be considered through the change control process.

12. The resources working on approved change requests shall be separate from the resources that were deployed under the original Scope of Work as per this RFP. MSP shall notify GeM about the details of the resources working on each change request via CR Form-2 and 3. The deployment schedule of these resources shall be mutually aligned between GeM & the MSP. Any changes being implemented by the resources deployed under the original Scope of Work as per this RFP shall not be treated as change requests.

8.7.7 APPENDIX

FORM I: Format for Change Request Notice (For In Principal Approval)

PART A: Requirement INITIATION (to be filled by GeM)	
CRN Number:	<<Prov CR/GeM/YYYY/Running Number (NNNN)>> (Initiator to take this number from PMU head)
Date:	DD/MM/YYYY
Title:	
Initiator:	Name of ACEO/DCEO/ PMU Member etc. who is initiating the CR

Category of Change:	<<Application Software / Infrastructure Procurement /Help Desk/Any Other>>
Brief Description of Proposed Change:	
Signature of initiator:	**Date:**

Note: the initiator will submit the change request to Nodal person/ PMU SPOC

CRN Number: <<Prov CR/GeM/YYYY/Running Number (NNNN)	Date:

Detailed Description of Change:

JIRA or equivalent software ID:

Documentation:

Impact: Explicitly mention the impact on

Application Modules Impacted:

Registration		Incident Management	
Category Mgmt.		Business Intelligence & Analytics	
Catalogue Mgmt.		Request Management System	
e-procurement		GeM Portal	
Contract Mgmt.		Admin Panel	
Fulfillment		LMS	
Payments		Others	

Databases Impacted: **Infrastructure Impacted:** **Other Impact:**	

Undertaking from MSP: Post analysis of Change Request, we undertake that, the change is beyond the Scope of Agreement between GeM and MSP including ancillary and concomitant services required and as detailed in the sign-off version of all required documents, including Agreement and BRDs.	
Any Other Relevant Information:	
Name of PD MSP	
Signature of PD MSP:	
Decision of CRMC	**Discussed on -------------------** **Final decision: Rejected/Approved**

Note:

1. MSP may discuss with initiator for any clarification on the Change Request.

2. MSP will have to attach all artefacts related to the development and justification of CR like previous BRD's, JIRA or equivalent software IDs and anything else which is relevant as annexure along with the form.

3. MSP to submit details of alternative options possible to address the change if any, the implications of these alternative options and reason for selecting particular option.

FORM II: Format for Change Request Notice (For Effort & Cost Calculation and Preliminary Approval)

PART A: INITIATION (Auto-filled by the tool)	
CRN Number: <<Number>>/A	**Date:**
Title:	
Initiator:	
Brief Description of Proposed Change: (To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Name & Designation: (On behalf of Initiator)	
Signature:	**Date:**

Part B : EVALUATION (For non-revenue generating change requests)	
CRN Number: <<Number[1]>>/B	**Date:**
Detailed Description of Change:	
Impact: Detailed impact analysis, impact on hardware/server/infra requirement, security clearance. Quantify any effects the proposed change will have on budgets of scarce resources, such as memory, processing power, network bandwidth, real-time schedule.	
Deliverables Involved:	
Detailed Timelines:	

---

[1] CRN Number will be same for both Parts, but demarcated with "/<Part Name>"

Effort Estimates and Cost/Charges for Proposed Change (not to be filled in case of Revenue Generating Change Request):

1. *Include detailed costing to arrive at such cost structure and schedule of payments, if change is approved*
2. *Detail the effort estimate for all resources working on change request, under the terms of this Agreement*
3. *Resource deployment plan (details of resources to be deployed on the change request)*

Impact/ Dependencies/ Inputs required from Service Recipient and/ or Third Party Suppliers:

Any Other Relevant Information:

1. *Detail the effect of the Proposed Change on the MSP's ability to meet each Milestone Date*

Name & Designation (On behalf of MSP)	
Signature:	**Date:**

Authority to Proceed: Implementation of this CRN as submitted in Part A, in accordance with Part B is: (tick as appropriate after receipt of final approval from the authority as designated in the Standard Operating Procedures and/or by the Competent Authority in GeM)

Approved Comments:	**Rejected** Comments:
For Government e-Marketplace	**For MSP**
Signature	Signature
Name:	Name:

Designation:	Designation:
Date:	Date:

FORM III: Format for Change Request Notice (For Actual Effort & Cost Calculation and Final Approval)

PART A: INITIATION (Auto-filled by the tool)	
CRN Number: <<Number[1]>>/A	**Date:**
Title:	
Initiator:	
Brief Description of Proposed Change: (To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Name & Designation: (On behalf of Initiator)	
Signature:	**Date:**

---

[1]

Part B : EVALUATION	
CRN Number: <<Number[1]>>/B	**Date:**

Detailed Description of Change:

Impact: Detailed impact analysis, impact on hardware/server/infra requirement, security clearance. Quantify any effects the proposed change will have on budgets of scarce resources, such as memory, processing power, network bandwidth, real-time schedule.

Deliverables Involved:
Detailed Timelines:

Resources Deployed, Actual Effort and Cost/Charges for Proposed Change (not to be filled in case of Revenue Generating Change Request):
1. *Resources deployed (Name, designation, etc.)*
2. *Include detailed costing to arrive at such cost structure and schedule of payments*
3. *Detail the actual effort for all resources working on change request, under the terms of this Agreement.*

Impact/ Dependencies/ Inputs received from Service Recipient and/ or Third Party Suppliers:

Any Other Relevant Information:
1. *Detail the effect of the Change on the MSP's ability to meet each Milestone Date*
2. *Any additional requirements provided by MSP to the change during implementation*

MSP Undertaking: This is to certify that all resources involved in the development of said functionality were separate from the resources that were deployed under the original Scope of Work as per this RFP.

Name & Designation (On behalf of MSP)	

---

[1] CRN Number will be same for both Parts, but demarcated with "/<Part Name>"

Signature:	Date:
Authority to Proceed: Implementation of this CRN as submitted in Part A, in accordance with Part B is: (tick as appropriate after receipt of final approval from the authority as designated in the Standard Operating Procedures and/or by the Competent Authority in GeM)	
Approved Comments:	**Rejected** Comments:
For Government e-Marketplace	**For MSP**
Signature	Signature
Name:	Name:
Designation:	Designation:
Date:	Date:

GOVERNMENT OF INDIA
MINISTRY OF COMMERCE & INDUSTRY

Government e-Marketplace

3rd floor, Jeevan Bharti Building, Janpath, Connaught Place,
New Delhi-110001

REQUEST FOR PROPOSAL

Selection of Managed Service Provider (MSP) for
Design, Development, Implementation,
Operation & Maintenance of
Government e-Marketplace (GeM)

RFP Number:

GeM/Hiring_Of_MSP/2022/01

Volume - 2: Instruction to bidders

Contents

List of Tables

ACRONYMS

Abbreviation	Description
GeM	Government e-Marketplace
AI	Artificial Intelligence
AMC	Annual Maintenance Contract
API	Application Programming Interface
App	Application
ATC	Average Total Cost
ATS	Atomic Test and Set Locking
BCP	Business Continuity Planning
BoQ	Bill of Quantity
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT-in	Indian Computer Emergency Response Team
CI/ CD	Continuous Integration and Continuous Delivery
CMMi	Capability Maturity Model Integration
CORS	Cross-Origin Resource Sharing
COTS	Commercial-Off-The-Shelf
CQRS	Command and Query Responsibility Segregation
Cr.	Crore
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CSPAF	CSP Authorization Form
CV	Curriculum Vitae
DB	Database
DC	Data Centre
DDoS	Distributed Denial of Service
Dev	Development
DR	Disaster Recovery
DRC	Disaster Recovery Center
EMD	Earnest Money Deposit

FY	Financial Year
GB	GigaByte
GST	Goods and Services Tax
GSTN	Goods and Services Tax Network
HIDS	Host-based Intrusion Detection System
IaaS	Infrastructure as a Service
IAS	Indian Administrative Service
IEM	Independent External Monitor
INR	Indian Rupee
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LLP	Limited Liability Partnership
LOA	Letter of Award
LOI	Letter of Intent
MBps	MegaBytes per second
MeiTY	Ministry of Electronics and Information Technology
ML	Machine Learning
MoU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Master Service Agreement
MSP	Managed Service Provider
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
O&M	Operations & Maintenance
OEM	Original Equipment Manufacturer
OS	Operating System
OSS	Operations Support System

P&L	Profit & Loss
PaaS	Platform as a Service
PBG	Performance Bank Guarantee
PKCE	Proof Key for Code Exchange
PO	Purchase Order
PSU	Public Sector Undertaking
QCBS	Quality Cost-Based Selection
RAM	Random Access Memory
Retd.	Retired
RFP	Request For Bid
RPO	Recovery Point Object
RTO	Recovery Time Object
SI	System Integration
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
SOC1	System and Organization Controls 1
SOC2	System and Organization Controls 2
SSL	Secure Sockets Layer
STQC	Standardisation Testing and Quality Certification
TB	TeraByte
TCV	Total Contract Value
TIA	Tax Injunction Act
UAT	User Acceptance Testing
UI	User Interface
UX	User Experience
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

Bid notification and data sheet table

#	Item	Description
1.1	Name of the Purchaser	Government eMarketplace
1.2	Tender Inviting Authority	CEO- GeM
1.3	Job Requirement	Selection of Managed Service Provider (MSP) for Design, Development, Implementation, Operation & Maintenance of Government e-Marketplace (GeM)
1.4	Method of Selection	The method of selection is Combined Quality and Cost Based Selection (QCBS). The weights given to the Technical and Commercial Bids are: Technical = 70% and Commercial = 30%
1.5	Tender Fee (Non-Refundable & Not Exempted)	Nil
1.6	Bid Security/ Earnest Money Deposit (EMD) with validity	INR 1.5 Cr. (One Crore Fifty Lakhs); EMD shall be valid for at least 180 (One Hundred and Eighty) days from the last date of submission of the Bid in the name of Government eMarketplace
1.7	Last date for Submission of Physical copy or Bid Security/ Earnest Money Deposit (EMD)	As per CPPP Portal

#	Item	Description
1.8	Availability of RFP Documents	CPPP Portal
1.9	Last date for download of RFP	As per CPPP Portal
1.10	Last date for Submission of Pre-Bid Queries	As per CPPP Portal
1.11	Pre-bid Conference: GeM System Walkthrough Time, Date, & Venue	10-10-2022 , 11:00 AM Venue- Constitution Club of India, Rafi Marg, Sansad Marg, behind RBI Bank, Sansad Marg Area, New Delhi, Delhi 110001
1.12	Pre-Bid Conference: Pre-bid meeting Time, Date, & Venue	19-10-2022 , 11:00 AM Venue- Constitution Club of India, Rafi Marg, Sansad Marg, behind RBI Bank, Sansad Marg Area, New Delhi, Delhi 110001
1.13	Date of Publishing of Responses to pre-bid queries Corrigendum by GeM	As per CPPP Portal
1.14	Last date and time for Bid/Bid submission (on / before)	As per CPPP Portal
1.15	Submission of Integrity Pact, EMD and Letter of Authorization (Physical hard copy submission)	As per CPPP Portal
1.16	Pre-Qualification Bid Opening - Time, Date, & Venue	As per CPPP Portal

#	Item	Description
1.17	Technical Bid Opening - Time, Date, & Venue	As per CPPP Portal
1.18	Date for Technical Presentation by Bidders	As per CPPP Portal
1.19	Date & time for Opening of Commercial Bids	As per CPPP Portal
1.20	Language of Bid Submission	English
1.21	Bid Validity	120 days
1.22	Currency	INR
1.23	Performance Bank Guarantee	3% of Total Contract Value; To be submitted within 15 (Fifteen) days of receipt of the notification of award for the amount with the validity up to duration of the contract and six months thereafter.
1.24	Name, contact details and Address for Communication and seeking clarifications	Shri Anuj Kumar, Director (Adm), GeM 3rd Floor, Tower II, Jeevan Bharti Building Connaught Place, New Delhi

Note: The above dates, time and venue may be altered by the Purchaser at its sole discretion with prior notice to the Bidders. Some of the information provided in the above Data Sheet is further elaborated in the subsequent sections of this RFP and the information provided in the Data Sheet and subsequent sections of this RFP are to be read in conjunction and interpreted harmoniously.

1. Instruction to Bidders

1.1 Eligible Bidders

Bids can be submitted by any organization that is reputed in the activities related to the design, development, implementation, operation, maintenance, and support of large-scale IT systems or e-marketplace application in India. Detailed criteria can be referred in Volume 2 Section 2.2 Pre-Qualification criteria of this RFP.

Consortium bids are allowed under this RFP. In case of a Consortium bid, the "Lead Bidder" will be responsible for meeting all obligations of the Consortium and the delivery of goods and services mentioned in all volumes of this RFP, including but not limited to:

1. The management of Consortium Partner who is also a part of the bid and for the delivery of all products and services in accordance with the Agreement

2. The supply, delivery and installation, commissioning of all products and providing all services as submitted in their bid

3. Ensuring the successful execution of integrated solution including meeting the SLAs as defined in Volume 1 Section 8.6 of this RFP.

The list of Consortium Partners needs to be declared in the bid. Any change in the Consortium during the bidding process will lead to disqualification of the Consortium. Bids submitted by a Consortium should comply with clauses related to the Consortium in Volume-3 of this RFP and following requirements:

1. The Lead Bidder shall be authorized to incur liabilities and receive instructions for and on behalf of any and all Consortium Partners;

2. A Consortium can have a maximum of 2 (Two) Consortium Partners apart from the Lead Bidder

3. Any entity can be a Lead Bidder OR a Consortium Partner in only 1 (One) bid submitted against this RFP

Internal arrangement between the Consortium Partners is left to the bidders, subject to relevant clauses in Volume-3 of this RFP. It is the responsibility of the Lead Bidder to ensure that the other Consortium Partners in the bid are compliant to all the clauses as mentioned in the bid, failing which bid can be disqualified. If, during the bidding process, the Consortium as proposed in the bid is dissolved or the Consortium Partners change, then the Bid is liable to be disqualified.

Sub-Contracting

Sub-Contracting under this RFP is allowed with the consent of the Purchaser, however, all the activities listed as part of the following sections of the Volume 1 of this RFP should not be sub-contracted by the Bidder:

1. Section 3.1.2: Application Design, Development, and Implementation (except development of Certificate Authority solution as detailed in Volume 1 Section 8.1.19 of this RFP)

2. Section 3.1.3: External Integrations

3. Section 3.1.6: Application Training and Capacity Building

4. Section 3.1.7: L1 and L2 resources (including agents, L1 & L2 Delivery Lead, Manager Operations, etc.) from Contact Center & Technical Helpdesk

5. Section 3.1.8: Operations and Maintenance

All resources deployed for the above mentioned activities (i.e. where sub-contracting is not permitted) must be on the pay-roll of the Bidder or Lead Bidder/ Consortium Partners (in case of a Consortium bid).

Furthermore, the bidder or Lead Bidder (in case of a Consortium bid) shall ensure that the resources from the Consortium Partner/ Sub-Contractor should be deployed only for the respective scope of work of the Consortium Partner / Sub-contractor

In case the Bidder wants to provide the services of the CSP itself, then it must also meet the pre-qualification criteria mentioned in the RFP for CSP. In case of sub-contracting of cloud provisioning services with a CSP, the bidder / Lead Bidder must enter into a Teaming Agreement outlining the scope and clear roles & responsibilities with the CSP and submit the same in the bid. Post successful award of the contract, MSP shall submit the contract between MSP and CSP. Commercials of the agreement may be masked for submission. Back-end MoUs may be executed between the parties provided such back end MoUs do not override the terms of the sub-contract agreement.

The Bidder / Lead Bidder shall be responsible for performance of its nominated sub-contractor(s). The Bidder needs to mention details of any sub-contracting proposed in the bid along with name of the sub- contractor and activity assigned as a self-certified declaration on the Lead Bidder's official letter head. Any change in subcontractor(s) at later date will be allowed only after approval of the Purchaser.

1.2 Bid Preparation Costs

The Bidder shall bear all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in the conduct of informative and other diligence activities, participation in meetings/ discussions/ presentations, preparation, and submission of the bid, in providing any additional information required by the purchaser to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process. The Purchaser

will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the entire Bidding Process.

1.3 Earnest Money Deposit (EMD)

1. The Bidders shall submit an EMD as bid security fee from a scheduled bank, in form of a Bank Guarantee, along with a signed and stamped copy of the Integrity Pact in a sealed envelope, of an amount and as per the details mentioned in this RFP. EMD in any other form will not be accepted. EMD must remain valid for at least 180 (One Hundred and Eighty) days from the last date of submission of the Bid and the validity of the EMD should be extended in the event the last date of submission of the Bid is extended. No interest will be payable by the Purchaser on the EMD.

2. Copy of the EMD instrument should be uploaded onto the CPPP Portal as a part of the Fee Cover submission and a physically signed copy of the same shall be submitted as per stipulated deadline mentioned in this RFP.

3. The EMD is required to protect the Purchaser against the risk of Bidder's conduct which may warrant EMD's forfeiture pursuant to the instances mentioned in Volume 2 Section 1.3 Clause (7) below.

4. EMDs of all unsuccessful Bidders will be returned, without interest, at the earliest after the expiry of the final bid validity and latest on or before the 30th (Thirtieth) day after the award of the contract under this RFP.

5. The EMD of the successful Bidder will be returned, without interest, upon submission of PBG by the successful Bidder as defined in Volume 2 Section 3.3 of this RFP.

6. In case the EMD is not received by the stipulated deadline then the Purchaser reserves the right to forthwith and summarily reject the Bid of the concerned Bidder without providing any opportunity for any further correspondence by the concerned Bidder.

7. The EMD may be forfeited:

    a. If a Bidder withdraws the bid or increases the quoted prices after the opening of the Bid and during the period of the Bid validity period or its extended period if any.

    b. In case of a successful Bidder, if the Bidder fails to sign the Agreement in accordance with the terms and conditions (including timelines for execution of the Agreement) of this RFP or fails to furnish the PBG in accordance with the terms and conditions (including timelines for furnishing PBG) of this RFP.

    c. If the bidder is found indulging in any corrupt, fraudulent, or other malpractice in respect of the bid;

> d. If the documents information provided by the bidder during the bid process is found to be incorrect, false, or misleading.

1.4 Integrity Pact

The Bidder is required to enter into an Integrity Pact with the Purchaser. For this, the Bidder shall submit an original signed and stamped Integrity Pact as a part of the Pre-Qualification Cover online and a physically signed copy of the same shall be sent as per stipulated deadline mentioned in this RFP. The format of the Integrity Pact shall be as provided in Volume-2 Section 4.3.7 of this RFP, failing which, the Bid submitted by the concerned Bidder will be liable to be forthwith and summarily rejected.

1.5 Pre-Bid Meeting & Clarifications

1.5.1 Bidders Queries

Any clarification regarding the RFP document and any other item related to this project can be submitted to the Purchaser as per the submission mode and stipulated timelines mentioned in this RFP. The pre-bid queries should be submitted in the format as mentioned in Volume 2 Section 4.1 of this RFP, along with the name and details of the Bidder submitting the queries. Any requests for clarifications received after the expiry of the date and timeline mentioned in this RFP shall not be entertained by the Purchaser. Further, the Purchaser reserves the right to issue or not issue any responses / clarifications / corrigendum at its own discretion.

1.5.2 Responses to Pre-Bid Queries and Issue of Corrigendum

The Purchaser will organize a pre-Bid Conference in two parts, 1. GeM System Walkthrough and 2. Pre-bid Meeting, as per stipulated timelines mentioned in this RFP and may respond to any request for clarifications and/or modifications of this RFP. It may formally respond to the pre-Bid queries after the Pre-Bid Meeting as mentioned in the RFP.

Upto 5 (Five) persons, duly authorized by the Bidder, will be allowed to participate in the system walkthrough and pre-bid meeting. For participation of more than 5 persons from a bidder, bidder can seek prior approval from GeM. The authorized representatives should carry valid proof of identification for verification before the commencement of the pre-Bid conference.

While the Purchaser will endeavor to provide a timely response to all the queries, the Purchaser makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does it undertake to answer all the queries that have been posed by the Bidders. Any modifications of this RFP, which may be necessary as a result of the pre-Bid Conference or for any other reason, shall be made available by the Purchaser exclusively through a corrigendum. Any such corrigendum shall be deemed to be incorporated into this RFP. However, in case of any such amendment of the RFP, the Bid submission date may be extended by the Purchaser at the sole discretion of the Purchaser.

All clarifications or any other corrigendum notification issued by the Purchaser subsequent to the issuance of this RFP will be published online as well as sent to the email ids specified by the organizations during pre-Bid conference.

1.6 Bid Validity Period

1. A bid shall remain valid for the time mentioned in the RFP.

2. The purchaser may request the Bidder(s) for an extension of the validity period of the bid up to 90 (Ninety) more days. Bidders will be required to extend the validity of the bids for such 90 (Ninety) days period. The validity of the EMDs as requested in the Volume 2 Section 1.3 of this RFP should also be suitably extended if called upon to do so by the purchaser. Bidders will have the right to refuse to extend the validity of bids beyond the said 90 (Ninety) days period and to withdraw the bids. The request and the responses thereto shall be made in writing (or by fax or email).

1.7 Submission of Bids

1. Bids shall be submitted online, and all the files uploaded by the bidders should have the file name in accordance with the [form_name.bidder_name] format. Bidder name should contain only the first two words of its name. The bid received in any other manner are liable to be summarily rejected.

2. Bids submitted by each potential bidder must contain following 4 (Four) components:

   a. Cover 1 (Fees)

   b. Cover 2 (Pre-Qualification)

   c. Cover 3 (Technical bid)

   d. Cover 4 (Commercial bid)

3. GeM will determine whether each Bid is responsive to the requirements of the RFP at each evaluation stage or not as indicated below. GeM may, in its sole discretion, summarily reject any Bid that is not responsive hereunder. A Bid should be considered responsive at each stage only if:

   a. **Fee**

      i. it is accompanied by the Earnest Money Deposit Format as specified in Volume 2 Section 4.2.1 of this RFP; and

      ii. it is received by the Proposed Due Date including any extension thereof

in terms hereof; and

iii.　it is not non-responsive in terms hereof

b. Pre-qualification Bid

i.　it is received by the Proposed Due Date including any extension thereof in terms hereof;

ii.　it does not contain any condition or qualification; and

iii.　it is not non-responsive in terms hereof

c. Technical Bid

i.　it is received by the Proposed Due Date including any extension thereof in terms hereof;

ii.　it does not contain any condition or qualification; and

iii.　it is not non-responsive in terms hereof

d. Commercial Bid

i.　The Financial Bid is received in the format as specified in Volume 2 Section 4.5.2 of this RFP;

ii.　it is received by the Proposed Due Date including any extension thereof in terms hereof;

iii.　it does not contain any condition or qualification; and

iv.　it is not non-responsive in terms hereof.

4. The Purchaser reserves the right to summarily reject any Bid which is non-responsive and no request for alteration, modification, substitution, or withdrawal will be entertained by the Purchaser in respect of such Bids. However, Purchaser reserves the right to seek clarifications or additional information from the bidders during the evaluation process.

5. If bidder on selection refuses to provide service, the bidder will be blacklisted by the Purchaser and will not be considered for any future work assignments.

6. No bids shall be accepted after the closing time for submission of bids.

7. After the bid submission until the grant of the work order, if any Bidder wishes to contact the Purchaser on any matter related to its bid, it should do so in writing at the bid submission

address. Any effort by the bidder to influence the Purchaser during the bid evaluation, bid comparison or grant of the work order decisions may result in the summarily rejection of the bid.

1.8 Bid Format

Bidder shall submit their bids in the formats prescribed in this RFP. Bids that are not in the prescribed formats will be liable to be summarily rejected. If a format for a specific document is not provided for in this RFP, the document shall be submitted in a format that makes it legally valid and binding on the Bidder and that is acceptable to the Purchaser. In any event, the Purchaser shall have the right to seek clarifications and modifications on the document submitted by the Bidder and the Bidder shall be obliged to provide such clarifications and modifications within the timelines specified by the Purchaser.

1.8.1 Fee Cover

#	Section Heading	Details
1.	EMD	Scanned copy of the EMD. Details in **Volume 2 Section 1.3** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*

Table 1: Fee Cover

1.8.2 Pre-Qualification Bid Cover

#	Section Heading	Details
1.	Pre-qualification Bid Covering Letter	As per the format provided in **Volume 2 Section 4.3.1** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*
2.	Integrity Pact	Scanned Copy of the Integrity Pact. Details in **Volume 2 Section 1.4** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*
3.	Profile of the Bidding Firms	As per the format provided in **Volume 2 Section 4.3.2** *(To be filled separately by Bidder/ Lead Bidder, Consortium Partner (if any) & Subcontractor(s) (if*

		any))
4.	Pre-Qualification Criteria	Pre-Qualification criteria table as mentioned in **Volume 2 Section 2.2** with response and reference against each criterion
5.	Power of Attorney/ Copy of Board Resolution	1. Power of Attorney executed by Lead Bidder in favor of Authorized Signatory signing the bid **(Volume 2 Section 4.3.9)** 2. Power of Attorney executed by Consortium Partners in favour of Lead Bidder **(Volume 2 Section 4.3.10)**
6.	Evidence of Sub-Contract	1. Self-certified declaration on the Bidder / Lead Bidder's official letter head with details of any sub-contracting proposed in the bid along with name of sub- contractor and activity assigned 2. Copy of the Pre-submission Teaming Agreement outlining the scope and clear roles & responsibilities 3. CSP Authorization Form **(Volume 2 Section 4.3.8)** *(to be filled by the Cloud Service Provider (CSP) of the solution proposed)*
7.	No Deviation Certificate	As per the format provided in **Volume 2 Section 4.3.5** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*
8.	Total Responsibility Certificate	As per the format provided in **Volume 2 Section 4.3.6** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*

Table 2: Pre-Qualification Cover

Note: The hardcopies of Integrity Pact, EMD, and Power of Attorney documents will have to be sent to address as mentioned in this RFP within the stipulated time as mentioned in this RFP.

1.8.3 Technical Bid Cover

#	Section Heading	Details
1.	Technical Evaluation Criteria	Technical Evaluation criteria table as mentioned in **Volume 2 Section 2.3** with response and reference against each criterion *(Format for Bidder's experience client citations to be filled separately by Bidder / Lead Bidder, Consortium Partner (if any) & Subcontractor(s) (if any))*
2.	Sizing for different Technical components	Format as per **Volume 2 Section 4.4.4** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*
3.	Project Plan	Format as per **Volume 2 Section 4.4.5** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*
4.	Details of Key Personnel proposed	CVs as per the format provided in **Volume 2 Section 4.4.6** *(to be provided by Bidder, or Lead Bidder on behalf of Consortium)*
5.	Bill of Quantities (BoQ)	Format as per **Volume 2 Section 4.4.7** *(to be provided by Bidder, or Lead Bidder on behalf of Consortium)*
6.	Other Supporting Documents	As applicable

Table 3: Technical Bid Cover

1.8.4 Commercial Bid Cover

#	Section Heading	Details
1.	Commercial Bid Covering Letter	As per the format provided in **Volume 2 Section 4.5.1**

2.	Commercial Bid and Cost summary of different solution components	As per the format provided in **Volume 2 Section 4.5.2** *(to be filled by Bidder, or Lead Bidder on behalf of Consortium)*

<div align="center">

Table 4: Commercial Bid Cover

</div>

The Bidders shall quote for the entire scope of contract on an "overall responsibility" basis such that the total contract value covers all obligations of the Bidder mentioned in or to be reasonably inferred from the Bidding documents in respect of providing the product services.

Prices quoted by the Bidder shall remain firm during the entire contract period and shall not be subject to variation on any account except change in applicable tax rates. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be summarily rejected.

1.9 Language

Bids should be filled by the bidders in the English language only. If any supporting documents submitted are in any language other than English, translation of the same in the English language should be duly attested by the Bidders. For the purpose of interpretation of any such documents, the English translation shall govern.

1.10 Authentication of Bids

The Authorized Signatory representing the Bidder shall digitally sign all Bid documents uploaded on CPPP Portal and submit a physically signed and stamped Integrity Pact, Letter of Authorization and the EMD. The Bid should be accompanied by authorization in the name of the signatory of the Bid. The authorization shall be in the form of a duly executed Power of Attorney (format provided in Volume 2 Section 4.3.9 of the RFP) or a Board resolution in favor of the person submitting the Bid in case the Bidder is a Company.

In case of a consortium bid, an additional authorization shall be required in the form of a duly executed Power of Attorney in favour of authorized representative of the Lead Bidder (format provided in Volume 2 Section 4.3.10 of the RFP).

1.11 Amendment of Request for Bid

At any time prior to the submission deadline of the bids, the Purchaser, for any reason, may modify the RFP by amendment and publish it. Such amendments shall be binding on the Bidders.

1.12 Compliant Bids: Completeness of Response

1. The Bidders are advised to study all instructions, forms, terms, requirements, and other information in this RFP carefully. Submission of the Bid will be deemed to have been done after careful study and examination of this RFP with full understanding of its implications.

2. Failure to comply with the requirements specified in this paragraph may render the Bid non-compliant and the Bid may be summarily rejected. Bidders must:

   a. Include all documentation specified in this RFP;

   b. Follow the format of this RFP and respond to each element in the order as set out in this RFP;

   c. Comply with all requirements as set out in this RFP.

3. Bids shall be submitted strictly in accordance with the requirements and terms & conditions of this RFP. The Bidder shall submit a No Deviation Certificate as per the format mentioned in Volume 2 Section 4.2.5 of this RFP. The Bids with deviation(s) shall be liable for summarily rejection of the bid.

1.13 Late Bids

The Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained. The Bids submitted by telex / fax /e-mail etc. shall not be considered. No correspondence will be entertained on this matter. The Purchaser shall not be responsible for any delay or non-receipt / non- delivery of the documents. No further correspondence on the subject will be entertained. The Purchaser reserves the right to modify and amend any of the above-stipulated conditions / criteria depending upon project priorities vis-à-vis urgent commitments.

Given that the bid submission has to be made online, it is advised that the Bidder takes all necessary precautions for the same, including submitting the Bid well in advance to avoid any last-minute hassles, ensuring that the names / formats of the files to be uploaded are as per the requirements, using the prescribed browser for upload etc. Purchaser shall not entertain any bids which could not be uploaded or uploaded properly in the portal for whatsoever reasons.

1.14 Right to Terminate the Process

The Purchaser may terminate the RFP process at any time and without assigning any reason. The Purchaser makes no commitments, express or implied, that this process will result in a business transaction with anyone. The Purchaser will not be liable in any way to any person in case of termination of this Bid process except that if the EMD has been received from the Bidder prior to such termination, the EMD will be returned (without any interest) as promptly as possible to the respective Bidders.

1.15 Non-Conforming Bids

A Bid may be construed as a non-conforming bid and ineligible for consideration if

1. It does not comply with the requirements of this RFP;

2. The bid appears to be "canned" presentations of promotional materials that do not follow the format required under this RFP or do not appear to address the particular requirements of the expected solution

1.16 Acceptance and Rejection of Bids

The Purchaser reserves the right to summarily reject any or all Bids without assigning any reason thereof. The Purchaser also reserves the right to assess the Bidder's capabilities and capacity. In either case, the decision of the Purchaser shall be final and binding. In the event of any assumptions, presumptions, key points of discussion, recommendation or any points of similar nature are submitted along with the Bids which amount to deviations in any form, the Purchaser reserves the right to seek withdrawal of such assumptions, presumptions, key points of discussion, recommendation, or any points of similar nature by the bidder. If the bidder does not withdraw such assumptions etc., the bid may be summarily rejected by GeM. If a discrepancy is found in a Bid, the same may be conveyed to the Bidder with a target date up to which the Bidder has to send his acceptance on the above lines and if the Bidder does not agree to the decision of the Purchaser the Bid is liable to be summarily rejected.

If the Bidder does not meet even one of the Pre-Qualification criteria as defined in Volume 2 Section 2.2 of this RFP, the Bidder shall be disqualified, and the entire Bid shall be summarily rejected.

1.17 Disqualification

The Bid is liable to be disqualified in, inter alia, any of the following cases or in case the Bidder fails to meet the bidding requirements as indicated in this RFP:

1. Bid not submitted in accordance with the terms, procedure and formats prescribed in this document or treated as a non-conforming bid;

2. During validity of the Bid, or its extended period, if any, the Bidder increases its quoted prices;

3. The Bidder's Bid is conditional and has deviations from the terms and conditions of RFP;

4. The Bid is received in incomplete form;

5. The Bid is received after the due date and time;

6. The Bid is not accompanied by all the required documents;

7. The Bid is submitted with a lesser validity period;

8. The information submitted in the Pre-Qualification is found to be misrepresented, incorrect or false, accidentally, unwittingly, or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period, if any;

9. The information submitted in the Technical Bid is found to be misrepresented, incorrect or false, accidentally, unwittingly, or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period, if any;

10. The Commercial Bid is enclosed within the Pre-Qualification or Technical Bid;

11. The Bidder tries to influence the bid evaluation process by unlawful / corrupt / fraudulent means at any point of time during the Bid process;

12. The bidder has otherwise been debarred by GeM or Department of Expenditure as on the date of submission of bid

13. In case any one party submits multiple bids or if common interests are found in two or more Bidders, the Bidders are likely to be disqualified, unless additional Bids / Bids are withdrawn upon notice immediately.

1.18 Fraud and Corrupt Practices

1. The Bidders and their respective officers, employees, agents, and advisers shall observe the highest standard of ethics during the selection process. Notwithstanding anything to the contrary contained in this RFP, the Purchaser shall summarily reject a Bid without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice (collectively the "Prohibited Practices") during the selection process. In such an event, the Purchaser shall, without prejudice to its any other rights or remedies, forfeit and appropriate the EMD or PBG, as the case may be.

2. Without prejudice to the rights of the Purchaser under Clause above and the rights and remedies which the Purchaser may have under the Agreement, if a Bidder is found by the Purchaser to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the selection process, or after the issue of the LOI or the execution of the Agreement, such Bidder shall not be eligible to participate in any tender or RFP issued by Purchaser during a period of 3 (Three) years from the date such Bidder is found by Purchaser to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

3. For the purposes of this Section, the following terms shall have the meaning hereinafter

respectively assigned to them:

a. "Corrupt Practice" means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the selection process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the Purchaser who is or has been associated in any manner, directly or indirectly with the selection process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the Purchaser shall be deemed to constitute influencing the actions of a person connected with the selection process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the selection process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/adviser of the Purchaser in relation to any matter concerning the Project;

b. "Fraudulent Practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the selection process;

c. "Coercive Practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the selection process;

d. "Undesirable Practice" means (i) establishing contact with any person connected with or employed or engaged by the Purchaser with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the selection process; or (ii) having a Conflict of Interest; and

e. "Restrictive Practice" means forming a cartel or arriving at any understanding or arrangement among the Bidders with the objective of restricting or manipulating a full and fair competition in the selection process.

1.19 Conflict of Interest

Any party involved in the preparation of this RFP is not allowed to bid. Further, any bidder who has or anticipates any conflict of interest with any of its current assignments while performing work under this RFP shall notify of the same to the Purchaser with a mitigation plan, within at most 3 (Three) weeks of the publication of this RFP and the Purchaser may decide whether to allow such bidder to bid or not.

2. Selection process for Bidders

2.1 Bid evaluation

1. Bids for this RFP will be evaluated based on Quality Cost-Based Selection (QCBS) method. The weightages for final technical score and commercial score will be 70:30 in this RFP.

2. Each of the Bids shall be evaluated as per the criteria and requirements specified in this RFP. As part of the evaluation, the bids submitted shall be checked to evaluate whether the bidders completely meet the prescribed Pre-Qualification Criteria.

3. Amongst the bids that meet the Pre-Qualification Criteria, Technical Bids will be opened, evaluated, and assigned a Technical score out of a maximum of 1000 (One Thousand) marks. **Only the bidders with an aggregate technical score of 60% or more will qualify for the commercial bid evaluation.** Failing to secure minimum marks will lead to technical rejection of the Bid on the portal. In addition, bidder shall also score **50% or more in each individual criteria of Technical Evaluation Framework**. Failure to score more than 50% in even one criteria of the framework will lead to technical rejection of the bid on the portal.

   The technical score achieved by the technically qualified Bidders will be normalized with the bidder with highest technical score taken as the base/ reference for arriving at Final Normalized Technical Score. Final Technical Score for each shortlisted bidder will be calculated as follows:

   a. Final Technical Score = (Technical score of the Bidder / Highest technical score awarded) * 100

4. Amongst the bids that meet the Pre-Qualification Criteria as well as secure minimum Technical score (Shortlisted bidders), Commercial bids will be opened. The bidding parameter value shall include all taxes, levies, duties, etc. (except Goods and Services Tax) as defined in Volume 1 Section 6 of this RFP. Commercial score for each shortlisted bidder will be calculated as follows:

   a. Commercial Score = (Minimum bidding parameter quoted / Bidding parameter quoted by the Bidder) * 100

5. Errors & Rectification: Arithmetical errors will be rectified on the following basis:

   a. If there is any discrepancy between words and figures, the amount in words will prevail for evaluation purposes

   b. If the Bidder does not accept the error correction, respective Bid shall be summarily rejected and EMD shall be forfeited

6. Purchaser reserves the right to appoint an Evaluation Committee for carrying out the

evaluation of the submitted bids basis defined criteria and scoring system in this RFP

7. Overall Final score, for each bidder, will be calculated as below:

   a. Final Score = (0.7 * Final Technical Score) + (0.3 * Commercial Score)

   b. The bidder with the highest Final Score shall be treated as the Successful Bidder

   c. In the event the Final scores are 'tied', the bidder securing the highest Final Technical score will be adjudicated as the Best Value Bidder for the award of the Project

2.2 Pre-Qualification Criteria

The Bidder's pre-qualification bid will be evaluated as per the following criteria:

#	Parameter	Pre-qualification criteria Description	Evidence required
1.	**Legal Entity**	The Bidder / Lead Bidder, Consortium Partner(s) (if any), **AND** all sub-contractors under this RFP, should be 1. A company incorporated in India under the Companies Act, 1956/ Companies Act, 2013 **OR** a Partnership Firm registered under the India Partnership Act, 1932 **OR** Limited Liability Partnership (LLP) registered under LLP Act, 2008 and subsequent amendments thereto 2. Registered with the Service Tax, and GSTN Authorities in India 3. Bidder / Lead Bidder and Consortium Partner(s) should have been in continuous existence **AND** operating in India for the last 7 (Seven) financial years (FY 2015-16, FY 2016-17, FY 2017-18, FY 2018-19, FY 2019-20, FY 2020-21, and FY 2021-22) 4. All sub-contractors should have been operating in India for the last 5 (Five) financial years (FY 2017-18, FY 2018-19, FY 2019-20, FY 2020-21, and FY 2021-22)	1. Copy of Certificate of Incorporation 2. Copy of Registration Certificates with the Service Tax, **AND** GSTN Authorities 3. For Bidder / Lead Bidder and Consortium Partner(s), Copy of audited Balance Sheets **AND** Profit & Loss Statements for the last 7 (Seven) financial years (FY 2015-16, FY 2016-17, FY 2017-18, FY 2018-19, FY 2019-20, FY 2020-21, and FY 2021-22) 4. For Sub-contractors, Copy of audited Balance Sheets **AND** Profit & Loss Statements for the last 5 (Five) financial years (FY 2017-18, FY 2018-19, FY 2019-20, FY 2020-21, and FY 2021-22) *The aforementioned documents shall be required*

#	Parameter	Pre-qualification criteria Description	Evidence required
			from each entity – Bidder / Lead Bidder, Consortium Partner (if any), and the sub-contractors participating in this RFP.
2.	**Sales Turnover**	1. **In case of a single bidder,** it should have an average annual revenue of at least **INR 1000 (One Thousand) Crores** in last 3 (Three) financial years (FY 2019-20, FY 2020-21, and FY2021-22) 2. In case of a Consortium bid: a. The Lead bidder should have an average annual revenue of at least **INR 700 (Seven Hundred) Crores** in last 3 (Three) financial years (FY 2019-20, FY 2020-21, and FY 2021-22) b. Each Consortium Partner should have an average annual revenue of at least **INR 300 (Three Hundred) Crores** in last 3 (Three) financial years (FY 2019-20, FY 2020-21, and FY 2021-22). c. Maximum of 2 (Two) Consortium partners are allowed in a Consortium bid. A Consortium partner can participate in only 1 (One) bid submitted against this RFP' 3. Average annual revenue to be considered from "IT system	1. Copy of audited Balance Sheets **AND** Profit & Loss Statements for the 3 (Three) financial years (FY 2019-20, FY 2020-21, and FY2021-22) 2. Duly filled Bidder's profile **(as per Volume 2 Section 4.3.2)** 3. In case the P&L Account shows consolidated revenues, then a Certificate from the Statutory Auditor / Company Secretary of the bidder is required to be submitted to corroborate the revenues of each entity *The aforementioned documents shall be required from each entity – Bidder / Lead Bidder and Consortium Partners (if any), participating in this RFP.*

#	Parameter	Pre-qualification criteria Description	Evidence required
		integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India or globally" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India or globally (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)" *(Note: For the purpose of this criterion, turnover excluding equipment and licensing will be considered while calculating this average annual revenue. Also, turnover of only the bidding entity will be considered. Turnover of any parent, subsidiary, associated or other related entity will not be considered.*	
3.	**Relevant Experience**	1. **In case of a single bidder,** it should possess experience with prior projects in any of the following areas – "IT system integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India or globally"" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India or globally (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)". The above project(s) should meet the following requirement in last 10	1. Citation as per format specified in **Volume 2 Section 4.3.3** **AND** any of the following: 2. Copy of Work Orders AND Completion Certificates from the client; **OR** 3. Copy of Work Order AND Phase Completion Certificate from the client;

#	Parameter	Pre-qualification criteria Description	Evidence required
		(Ten) financial years (FY 2011-2022):	**OR**
		a. At least 1 (One) such projects each of TCV of INR 400 (Four Hundred) Cr or more **OR**	4. Copy of client certificate as documentary proof for the stated criteria and implementation status;
		b. At least 2 (Two) such projects each of TCV of INR 200 (Two Hundred) Cr or more **OR**	**OR**
		c. At least 4 (Four) such projects each of TCV of INR 100 (One Hundred) Cr or more	5. Certificate by the Company Secretary of the bidder for the stated criteria and implementation status.
		2. **In case of a Consortium bid,** the Lead Bidder and Consortium Partners, together, should possess experience with prior projects in any of the following areas – "IT system integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India or globally" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India or globally (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)".The above project(s) should meet the following requirement in the last 10 (Ten) financial years (FY 2011-2022):	*Note 1 – In case of an integrated project, relevant certificate from the Statutory Auditor confirming value of relevant work to be submitted.* *Note 2 – All the projects cited should be in the name of the bidding entity and not in name of any parent, subsidiary, or affiliate entity.* *Note 3 – All the supporting documents mentioned above shall be required from all the bidding entities (Bidder / Lead Bidder / Consortium Partners) as*

#	Parameter	Pre-qualification criteria Description	Evidence required
		a. At least 1 (One) such projects each of value of INR 400 (Four Hundred) Cr or more **OR** b. At least 2 (Two) such projects each of value of INR 200 (Two Hundred) Cr or more **OR** c. At least 4 (Four) such projects each of value of INR 100 (One Hundred) Cr or more	*applicable.*
4.	**Certifications**	The Single Bidder, or in case of a consortium, any one of the Consortium Partners (including Lead Bidder) should possess valid CMMi Level 5 certificate **AND** any one of ISO 9001: 2008 / ISO 27001:2005 / ISO 20000 or later certificate valid as on the date of submission of the bid.	1. Copy of the valid requisite certificates *The aforementioned documents shall be required from relevant entity – Bidder / Lead Bidder or Consortium Partner*
5.	**Blacklisting**	Any of the Bidder / Lead Bidder, Consortium Partner (if any), **AND** sub-contractor under this RFP should not have been blacklisted/ suspended and should not be under a declaration of ineligibility for corrupt or fraudulent practices by GeM **OR** Department of Expenditure as on the date of submission of bid.	1. Self-certificate letter undertaking to this effect on company's letter head signed by the company's authorized signatory **(Volume 2 Section 4.3.4)** *The aforementioned documents shall be required from each entity – Bidder / Lead Bidder, Consortium Partner (if any), and the sub-contractors participating in*

#	Parameter	Pre-qualification criteria Description	Evidence required
			this RFP.
6.	**Cloud Infrastructure as a Service (IaaS) capabilities**	The Bidder **OR** Lead Bidder **OR** any of the Consortium Partner(s) should have Cloud Infrastructure as a Service (IaaS) capability, either in-house or through sub-contracting with a Cloud Service Provider (CSP), **AND** meet all of the following eligibility requirements: 1. **MeiTY empanelment**: The Bidder / Lead Bidder (in Consortium bid) **OR** the sub-contracted CSP should be MeiTY empaneled for provisioning of Government Community Cloud **OR** Virtual Private Cloud services 2. **Revenue:** The Bidder / Lead Bidder **OR** any of the Consortium Partner(s) **OR** the sub-contracted CSP (as a single legal entity or its holding company) must have an average annual revenue of **at least INR 100 (Hundred) Crores** from the Data Centre related services in India or globally in last 3 (Three) financial years (FY 2019-20, FY 2020-21, FY2021-22) 3. **IaaS Service Offering:** The Bidder / Lead Bidder **OR** any of the Consortium Partner(s) **OR** the sub-contracted CSP (as a single legal entity or its holding company) should be currently delivering IaaS	1. Proof of empanelment by MeiTY 2. Copy of Audited Balance Sheets, **AND** Profit & Loss Statements of the CSP along with Certificate from Company Secretary of the CSP, for last three financial years (FY 2019-20, FY 2020-21, FY 2021-22) In case the consolidated P&L account or In-house IaaS capabilities, then a Certificate from the Statutory Auditor / Company Secretary of the bidder / Consortium partner to be submitted to corroborate the revenues of the Data Centre related services. 3. CSP Authorization Form, as applicable **(Volume 2 Section 4.3.8)**

#	Parameter	Pre-qualification criteria Description	Evidence required
		services [as per the National Institute of Standards and Technology (NIST) Definition of Cloud Computing and providing on-demand Storage and VMs], since last 3 (Three) financial years (FY 2019-2022) in India. The IaaS offering shall provide for tools or capabilities that enable users to unilaterally provision, order, manage, and use the Cloud services: a. Service Management & Provisioning (Service Provisioning and De-Provisioning within near real-time of provisioning request, defined SLA Management, and Utilization Monitoring) b. Provide visibility into service via dashboard c. User /Admin Portal / User Profile and Trouble Management d. Cloud services should be accessible via internet and MPLS 4. **Data Centre (DC) & Disaster Recovery (DR) facility:** The DC Facilities one or more, as applicable, facilities from where the cloud service offerings are proposed to be offered, must meet the following criteria:	4. Copy of Agreement between MSP and CSP, as applicable 5. Copy of the valid requisite Certifications – Tier-III standard, ISO 27001, ISO 20000:1 for NOC 6. Documentary evidence of DC & DR locations where GeM Solution will be hosted and their distance from each other. 7. Self-certification by the bidder / Consortium partner / CSP (on its letter head) for eligibility requirements in IaaS service offerings and DC & DR facilities. *The Bidder / Lead bidder (in case of consortium) shall provide the following documents, either in-house or from the CSP, for compliance with the eligibility criteria.*

#	Parameter	Pre-qualification criteria Description	Evidence required
		a. The DC and DR should be placed in such a way that compute and related components can be used in Active-Passive configuration	
		b. The Data Centre Facility must be within India (at the time of deployment), should be currently operational, and have a minimum capacity of 50 (Fifty) Racks being operational in India (across all DCs owned and managed by the bidding entity)	
		c. Dedicated DR should be available in India	
		d. DC & DR should be provided by the same entity, should be Tier-3 or higher, and DC – DR locations should be at least at a distance of 100 kms from each other. DC – DR locations and distance between them should be specified at the time of bidding.	
		e. The DC Facilities shall at a minimum have: i. Routers, Firewalls, LAN, WAN, Internet Access, and Hosting	

#	Parameter	Pre-qualification criteria Description	Evidence required
		Centres, Backup, Operations Management, and Data Management	
		ii. Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Web-Application Firewall, Multi-Factor Authentication, VPN, IPS, Log Analyzer Syslog, SSL, DDOS Protection (layer 3 (Three) as well as layer 7 (Seven) and not just plain DDOS), HIDS, NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)	
		iii. Conform to at least Tier III standard, preferably certified under TIA 942 or	

#	Parameter	Pre-qualification criteria Description	Evidence required
		Uptime Institute certifications by a 3rd (Third) party	
		iv. Assured protection with security built at multiple levels	
		v. Certified for the latest version of ISO 27001	
		vi. NOC offered for the Data Centre and the managed services quality should be certified for ISO 20000:1 or above	
		vii. Carrier-neutral Data Centre viz; Multiple Connectivity service providers should be there	

Table 5: Pre-Qualification Criteria

Note: In case any Bidder / Lead Bidder or Consortium partner(s) has undergone corporate restructuring (including merger, demerger, hive off, slump sale etc.) in the last three financial years (FY 2019-20, 2020-21, 2020-22), it should showcase credentials of its erstwhile / current entity provided sufficient documentary proof is submitted with the undertaking to evince that such credentials have been transferred to the bidding entity and the bidding entity is authorized to use such credentials. Notwithstanding the foregoing, credentials of the parent entity, holding entity, subsidiaries or affiliates etc. cannot be used (and shall not be considered) unless such parent entity, holding entity, subsidiaries, or affiliates etc. is itself bidding in this RFP.

Note: All the citations that have to be provided for pre-qualification criteria shall be as per the format in **Volume 2 Section 4.3.3**.

Note: In case audited balance sheets and Profit & Loss Statements for FY2021-22 are not available for any entity, same can be replaced with audited balance sheets and Profit & Loss Statements for the year preceding to the earliest FY in consideration, as applicable.

2.3 Technical Evaluation Framework

Technical solution proposed by each bidder will be evaluated as per the criteria mentioned in the table below:

#	Evaluation Criteria	Total Marks	Minimum qualifying marks
1.	Bidder's Experience related to the assignment	400	>=200 (50% or more)
2.	Technical presentation and proposed solution	300	>=150 (50% or more)
3.	Resource Planning, Project Governance & Key personnel proposed	300	>=150 (50% or more)
TOTAL		**1000**	**>=600 (60% or more)**

Table 6: Technical Evaluation Framework

GeM reserves the right to check / validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the Bidder. The following sections explain how the Bidders will be evaluated on each of the Technical evaluation criteria.

2.3.1 Bidder's experience

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
1.	**Relevant Experience**	1. **In case of a single bidder,** it should possess experience with prior projects in any of the following areas – "IT system integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India or globally" **OR** "Development, implementation, and/or maintenance of an	1. Citation as per format specified in **Volume 2 Section 4.4.2** **AND** any of the following: 2. Copy of Work Order AND Completion	200

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		e-commerce / e-marketplace application in India or globally (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)". The above project(s) shall be **at least INR 300 (Three Hundred) Cr.** in last 10 (Ten) financial years (FY 2011-2022): a.3 (Three) citations (at least 1 should be successfully completed) = 160 (One Hundred and Sixty) marks, b. 2 (Two) citations (at least 1 should be successfully completed) = 120 (One Hundred and Twenty) marks, c.1 (One) citation (successfully completed) = 80 (Eighty) marks, d. 20 (Twenty) additional marks if one of the above citations is done for Central / State Government / Public Sector Undertaking / Public Sector Banks in India e.40 (Forty) additional marks if two of the above citations is done for Central / State Government / Public Sector Undertaking / Public Sector Banks in India	Certificates from the client; **OR** 3. Work Order AND Phase Completion Certificate from the client; **OR** 4. Copy of client certificate as documentary proof for the stated criteria and implementation status; **OR** 5. Certificate by the Company Secretary of the bidder for the stated criteria and implementation status. *Note 1 – In case of an integrated project, relevant certificate from the Statutory Auditor confirming*	

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		2. **In case of a Consortium bid,** the Lead Bidder and Consortium Partners, together, should possess experience with prior projects in any of the following areas – "IT system integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India or globally" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India or globally (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)". The above project(s) shall be **at least INR 300 (Three Hundred) Cr.** within last 10 (Ten) financial years (FY 2011-2022): a. 3 (Three) citations (at least 1 (One) should be successfully completed) = 160 (One Hundred and Sixty) marks, b. 2 (Two) citations (at least 1 should be successfully completed) = 120 (One Hundred and Twenty) marks, c. 1 (One) citation (successfully completed) = 80 (Eighty) marks, d. 20 (Twenty) additional marks if one of the above	*value of relevant work to be submitted.* *Note 2 – All the projects cited should be in the name of the bidding entity and not in name of any parent, subsidiary, or affiliate entity.* *Note 3 – All the supporting documents mentioned above shall be required from all the bidding entities (Bidder / Lead Bidder / Consortium Partners) as applicable.*	

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		citations is done for any Central / State Government / Public Sector Undertaking / Public Sector Banks in India e. 40 (Forty) additional marks if two of the above citations is done for Central / State Government / Public Sector Undertaking / Public Sector Banks in India		
2.	**Experience in IaaS capabilities**	The experience of the Bidder / Lead bidder / Consortium partners / CSP in provisioning IaaS and Platform as a Service (PaaS) for clients in India or globally. The above project(s) shall **be at least INR 20 (Twenty) Cr.** in last 10 (Ten) financial years (FY 2011-2022): 1. 4 (Four) or more projects = 80 (Eighty) marks 2. 3 (Three) projects = 60 (Sixty) marks 3. 2 (Two) projects = 40 (Forty) marks 4. 1 (One) project = 20 (Twenty) marks 5. 10 (Ten) additional marks if one of the above citations is done for Central / State Government / Public Sector Undertaking / Public	1. Citation as per format specified in **Volume 2 Section 4.4.2** **AND** any of the following: 2. Copy of Work Order AND Completion Certificates from the client; **OR** 3. Work Order AND Phase Completion Certificate from the client; **OR** 4. Copy of client certificate as	100

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		Sector Banks in India 6. 20 (Twenty) additional marks if two of the above citations is done for Central / State Government / Public Sector Undertaking / Public Sector Banks in India	documentary proof for the stated criteria and implementation status; **OR** 5. Certificate by the Company Secretary of the CSP for the stated criteria and implementation status. *Note 1 – In case of an integrated project, relevant certificate from the Statutory* Auditor *confirming value of relevant work to be submitted.* *Note 2 – All the projects cited should be in the name of the Bidder / Lead bidder / Consortium partners / CSP (as applicable) and not in name of any parent, subsidiary, or affiliate entity*	
3.	**Sales Turnover**	1. In case of a **single bidder**, average annual revenue in last 3 (Three) financial years (FY 2019-20, FY	1. Copy of audited Balance Sheets AND Profit &	100

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		2020-21, and FY2021-22) from "IT system integration, Application design, development and maintenance, data centre or cloud operations, and managed business services in India" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)" will be considered for evaluation as per the following slabs: a. Avg. Revenue > INR 1000 (One Thousand) Cr = 100 (One Hundred) marks b. INR 500 (Five Hundred) Cr < Avg. Revenue <= INR 1000 (One Thousand) Cr = 85 (Eighty Five) marks c. INR 200 (Two Hundred) Cr < Avg. Revenue <= INR 500 (Five Hundred) Cr = 70 (Seventy) marks 2. In case of a **Consortium bid**, total average annual revenue of Lead Bidder and Consortium Partners, together, in last 3 (Three) financial years (FY 2019-20, FY 2020-21, and FY2021-22) from "IT system integration, Application design, development and maintenance, data centre or cloud operations,	Loss Statements for the 3 financial years (FY 2019-20, FY 2020-21, and FY2021-22) 2. In case the P&L Account shows consolidated revenues, then a Certificate from the Statutory Auditor / Company Secretary of the bidder is required to be submitted to corroborate the revenues of each entity *The aforementioned documents shall be required from each entity – Bidder / Lead Bidder and Consortium Partners (if any), participating in this RFP.*	

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		and managed business services in India" **OR** "Development, implementation, and/or maintenance of an e-commerce / e-marketplace application in India (both internal and client projects allowed in case of e-commerce/ e-marketplace solution)" will be considered for evaluation as per the following slabs: a. Avg. Revenue > INR 1000 (One Thousand) Cr = 100 (One Hundred) marks b. INR 500 (Five Hundred) Cr < Avg. Revenue <= INR 1000 (One Thousand) Cr = 85 (Eighty Five) marks c. INR 200 (Two Hundred) Cr < Avg. Revenue <= INR 500 (Five Hundred) Cr = 70 (Seventy) marks *(Note: For the purpose of this criterion, turnover excluding equipment and licensing will be considered while calculating this average annual revenue. Also, turnover of only the bidding entity will be considered. Turnover of any parent, subsidiary, associated or other related entity will not be considered.)*		
	TOTAL			**400**

Table 7: Bidder's experience

2.3.2 Technical presentation and proposed solution

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
1.	**Overall e-Commerce marketplace solution**	Overall e-Commerce marketplace Solution including, but not limited to the following modules: 1. Seller's Management a. Seller's Services Lifecycle Management b. Catalogue Management c. Seller's Exit Management 2. Buyer's Management a. Buyer's Lifecycle Management b. Buyer's Registration c. Demand Aggregation d. Rating & Feedback 3. Catalogue Management a. Specifications Creation b. Product Photographs c. Update cycle 4. Logistics Management a. Dispatch & Delivery b. End to End Tracking c. Goods Return Management 5. Payment Gateway a. Integration with Buyers & Sellers	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		b. Settlement & Reconciliation 6. E-Tendering a.Direct purchase and L1 buy cycle b. End-To-End Process of E-Tendering c.Bid Process Management d. Security Compliance e.Document Management including Archival methodology 7. Finance & Administration Module a.Inter-departmental/Govt. Communication b. Accounting Methodology 8. End-To-End Product Lifecycle Management including but not limited to Workflow Management, User Management & Exit Management		
2.	**Overall Solution Architecture**	Domain driven architecture, Application architecture, Integration architecture, & Infrastructure deployment proposed and presentation covering at minimum the below key aspects: 1. Modularity and cohesiveness of the system 2. Scalability to handle future load by adding additional compute, storage automatically and no	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		constraints on the application		
		3. Suitability of Tools/Components & Technologies proposed including capacity to handle large volumes		
		4. How the system is compliance to architecture principles as required for GeM System – multilingual, multitenant		
		5. Approach to develop the API based system		
		6. Managing the API eco system		
		7. Approach for interfacing with other systems		
		8. Risk and mitigation Plan		
		9. Plan to handle multiple stakeholders		
3.	**Open Source**	Use of Open standards and open-source products	Bid and presentation	30
4.	**Cloud Architecture**	Cloud Architecture including 1. Data Centre Tier Classification 2. Number of ISP's present in the Data Centre 3. Capacity: Typical number of servers in a data centre dedicated for offering cloud services	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		4. Expansion Capability		
		5. Business Continuity Planning (BCP)		
		6. Dedicated Disaster Recovery Site		
		7. Dedicated and Redundant NOC and SOC		
		8. Proposed Uptime availability, RTO, RPO, and other offered SLAs for cloud services		
		9. Strong Governance Processes: Availability of services for the government department to regularly monitor cloud security posture, approaches, and usage		
		10. Dedicated and Redundant NOC and SOC		
		11. Security Compliances: Third Party security certifications, SOC1, SOC2		
		12. ISO 27017, ISO 27018		
		13. BCP Architecture: Architecture for providing Business Continuity / Disaster Recovery for meeting the RPO / RTO requirements specified in the RFP		
5.	**Security Architecture**	Security Architecture including: 1. Access & Identity Management – Tokens and grants with additional security for client	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		requests using PKCE 2. Application Security 3. Database security including ensuring nonrepudiation of data and reconstruction of truth 4. Governance framework to cover the threat landscape 5. Solution to ensure fool proof security to the system from various threats including hacking attempts, internal threats, etc. 6. Privilege management 7. Compliance to Regulations (IT Act, CERT-in and other government guidelines) 8. Security of payment gateways Have a cyclic of application software patch upgrades for an inbuild security product support		
6.	**Database Architecture**	Scalability of data architecture using - Data persistence patterns 1. Database as a service design 2. Event data store 3. API segmentation 4. CQRS pattern for maintaining data integrity	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
		5. Data schema's		
		6. Database security for any data change		
		7. Data governance mechanism including master data management		
		8. Ability for data architecture to support advanced analytics and AI use cases		
		9. Database security		
7.	**Understanding of GeM and Scope of work**	1. Level of understanding demonstrated for the GeM business processes and scope of work Understanding of the international software development best practices, risks & mitigation, and master data management	Bid and presentation	30
8.	**Approach & methodology for new platform development**	Approach for development and implementation of new platform and methodology for performing the required services as detailed in scope of work in the RFP and to meet the desired SLAs 1. Project management 2. Quality management 3. Reporting 4. Continuous improvements 5. Change management 6. Risk management	Bid and presentation	30

#	Citation	Areas to be demonstrated	Documentary Evidence	Max. marks
9.	**Approach & methodology for O&M of existing GeM platform**	Approach for ensuring operations, agreed enhancements & maintenance support for existing GeM portal including Knowledge Transfer plan, resource deployment & augmentation plan, etc.	Bid and presentation	30
10.	**Plan for transition / Refactoring, Migration, Upgradation, & Maintenance of new GeM portal post Go-Live**	Approach for new system enhancement / upgradation & maintenance of new refactored GeM portal including Knowledge Transfer plan, resource deployment & augmentation plan, operation & maintenance plan, etc.	Bid and presentation	30
	TOTAL			**300**

Table 8: Technical presentation and proposed solution

2.3.3 Resource Deployment Plan and Team Composition

For a project of such a large scale and complexity, it is imperative that the bidder should deploy best of class professionals to ensure successful execution of this project. The bidder, in its bid, should include the names and detailed CVs of their key personnel who will be working full time on this project, as per the table given below (in the CV Pro-forma as given in **Volume 2 Section 4.4.6**). Details around minimum educational and professional qualifications for each role, as provided below, are provided in **Volume 1 Section 8.5.2** of this RFP. Each named personnel shall be evaluated basis a combination of in-person interview and CV around the following parameters:

1. Educational qualifications

2. Quality of overall experience

3. Experience in similar assignments

4. Certifications

#	Profile/ Position	Number of named resources	Marks per resource	Total Marks
1.	Project Director - GeM	1	40	40
2.	Technical Program Manager	1	30	30
3.	Enterprise architect	1	40	40
4.	Solution architect	1	40	40
5.	Product manager	2	15	30
6.	Scrum Master	1	15	15
7.	DevOps Engineer	1	15	15
8.	Security Expert	1	15	15
9.	UI/UX Lead	1	15	15
10.	Business analyst / Domain Expert	2	15	30
11.	Data migration and cutover Expert	1	15	15
12.	AI/ ML Expert	1	15	15
	TOTAL	**14**		**300**

Table 9: Resource Deployment Plan and Team Composition

Note: The technical presentation is to be delivered in-person by the bidder's nominated Project Director and other 13 (Thirteen) team members as defined above only. The project sponsor from the bidder's organization shall also be present during the presentation, as deemed fit by the bidder. Virtual presentations and interviews shall be allowed in case of emergency with prior approval of GeM. The resources interviewed by GeM during evaluation phase must be the same on Day 1 (One) of the project, i.e. signing of MSA/ contract. Bidder must commit 100 (Hundred) per cent time availability of the above-named personnel since Day 1 (One) of the project. Replacement of any of the above-named personnel on or after the date of Technical Presentation shall result in levying of Liquidated Damages as defined in Volume 1 Section 3.3.3 of the RFP. The liquidated damages shall not be applicable if replacement of resource is required due to approved leaves by the MSP and GeM on account of maternity leave, or paternity leave, or serious medical conditions certified by a reputed medical practitioner and approved by GeM, or demise of the resource. Resources must be replaced with a resource of equal or higher competence. The replacement of the resource shall be interviewed by GeM prior to the final hiring.

Note: Wherever there is a problem in providing the name or cost of the project due to non-disclosure agreements with the clients, the bidder should provide a certificate from an independent auditor or Company Secretary. The bidder has to provide an undertaking with that to this effect.

Note: In case audited balance sheets and Profit & Loss Statements for FY2021-22 are not available for any entity, same can be replaced with audited balance sheets and Profit & Loss Statements for the year preceding to the earliest FY in consideration, as applicable.

3. Award of contract

3.1 Notification of Award

The Purchaser will notify the successful Bidder in writing that its bid has been accepted.

3.2 Signing of Contract

Within 21 (Twenty One) days of the receipt of the notification of award, the successful bidder shall execute the MSA as provided in Volume 3 of this RFP. Before the execution of the agreement (within 15 (Fifteen) days of receipt of the notification of award), the successful Bidder shall also submit the PBG in accordance with the terms in Volume 2 Section 3.3 of this RFP. If the successful bidder fails to execute the MSA within 21 (Twenty One) days or furnish the PBG within such 15 (Fifteen) days period (or such other extended timelines as agreed by the Purchaser at its sole discretion), Purchaser shall have the right to forfeit the EMD of the successful bidder and take any further action as deemed fit by the Purchaser, including blacklisting/ suspension of the bidder as per the applicable guidelines/ directives.

3.3 Performance Bank Guarantee (PBG)

The Purchaser will require the selected bidder to provide, at its own expense, an unconditional, irrevocable, and continuing PBG from a scheduled bank in India, in the format prescribed in Volume 2 Section 4.6 of this RFP. PBG shall be provided by the selected bidder within 15 (Fifteen) days from the date of the receipt of the notification of award, for a value equivalent to 3% of the total estimated contract value as mentioned in this RFP. PBG should be valid till the completion of the project and 6 (Six) months beyond expiry of the duration of this contract.

PBG shall contain a claim period of six months from the last date of validity. The selected Bidder shall be responsible for extending the validity date and claim period of the PBG as and when it is due on account of non-completion of the project and Warranty period. In case the selected Bidder fails to submit a PBG within the time stipulated, the Purchaser at its discretion may cancel the order placed to the selected Bidder without giving any notice. Purchaser shall invoke the performance guarantee in case the selected bidder fails to discharge their contractual obligations during the period, or the Purchaser incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.

Except as otherwise provided in Volume-3 of this RFP, no interest shall be payable on the PBGs. In case the project is delayed beyond the duration of this contract as defined in Volume 3 Section 3 of this RFP, the performance bank guarantee shall be accordingly extended by the Bidder till completion of the scope of work as mentioned in RFP Volume 1 and six months thereafter.

3.4 Failure to agree with the Terms & Conditions of the RFP

Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event GeM may award the contract to the next best value bidder or call for new bids. In such a case, GeM shall invoke the PBG and/or forfeit the EMD.

4. Annexures

4.1 Annexure-1: Template for Pre-Bid Queries

Bidder shall submit all pre-bid queries in excel in the following format.

#	Volume No.	Page No.	Section (Name & No.)	Statement as per RFP document	Query by bidder	Reason for Query
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Table 10: Template for Pre-Bid Queries

4.2 Annexure-2: Formats for Submission of the Fee

4.2.1 Bank Guarantee Format for Earnest Money Deposit (EMD)

To,

Director-Administration

3ʳᵈ floor Tower II

Jeevan Bharti Building, CP

New Delhi, 110001

Director-gem@gem.gov.in

Whereas **<<Name of the bidder>>** (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP # **<<RFP Number>>** dated **<<Date>>** for **<<Name of the assignment>>** (hereinafter called "the Bid") to **<<Nodal Agency>>**

Know all Men by these presents that we **<<Name of the bidder>>** having our office at **<<Address>>** (hereinafter called "the Bank") are bound unto the **<<Nodal Agency>>** (hereinafter called "the Purchaser") in the sum of Rs. **<<Amount in figures>>** (Rupees <<Amount in words>> only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this **<<Date>>**

The conditions of this obligation are:

1. If a Bidder withdraws the bid or increases the quoted prices after the opening of the Bid and during the Bid validity period or its extended period if any.

2. In case of a successful Bidder, if the Bidder fails to sign the Agreement in accordance with the terms and conditions (including timelines for execution of the Agreement) of this RFP or fails to furnish the Performance Bank Guarantee in accordance with the terms and conditions (including timelines for furnishing PBG) of this RFP.

3. If the bidder is found indulging in any corrupt, fraudulent, or other malpractice in respect of the bid; or

4. If the documents information provided by the bidder during the bid process is found to be

incorrect, false, or misleading.

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of the conditions mentioned above and specifying the occurred condition or conditions.

This guarantee will remain in force up to **<<insert date>>** and including **<<extra time over and above mandated in the RFP>>** from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN:

I.   Our liability under this Bank Guarantee shall not exceed Rs. **<<Amount in figures>>** (Rupees **<<Amount in words>>** only)

II. This Bank Guarantee shall be valid up to **<<insert date>>**)

III. It is a condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before **<<insert date>>**) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank) Seal:

Date:

4.3 Annexure-3: Formats for Submission of the Pre-Qualification Bid

4.3.1 Pre-Qualification Bid Covering Letter

<Location, Date>

Government e-Marketplace,
3rd floor,Tower II, Jeevan Bharti Building, Sansad Marg
New Delhi-110001
RFP dated *[date]* for selection for Managed Service Provider

Sir,

With reference to your RFP Document dated ***<date>***, we, the undersigned, having examined all relevant documents and understood their contents, offer to provide Design, Development, Implementation, Operation & Maintenance services for Government e-Marketplace (GeM) with reference to your Request for Bid dated ***<insert date>*** and our Bid. We are hereby submitting our Pre-qualification and Technical bid for selection as Managed Service Provider. We are submitting our Bid as ***<name of the bidder>***. The Bid is unconditional and unqualified.

We hereby declare that all the information and statements made in Pre-qualification bid are true and accept that any misinterpretation contained in it may lead to our disqualification. If negotiations are held during the period of validity of the Bid, we undertake to negotiate in accordance with the RFP. Our Bid is binding upon us in accordance with the RFP.

We understand that you are not bound to accept any Bid you receive. Further:

1. We acknowledge that Purchaser will be relying on the information provided in the Bid and the documents accompanying the Bid for selection of the Managed Service Provider, and we certify that all information provided in the Bid and in the supporting documents is true and correct, nothing has been omitted which renders such information misleading; and all documents accompanying such Bid are true copies of their respective originals.

2. This statement is made for the purpose of appointment as the Managed Service Provider for the aforesaid Project.

3. We shall make available to Purchaser any additional information it may deem necessary or require for supplementing or authenticating the Bid.

4. We acknowledge the right of Purchaser to summarily reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any

account whatsoever.

5. We declare that:

    a. We have examined and have no reservations to the RFP, including any Addendum issued by the Purchaser;

    b. We do not have any conflict of interest in accordance with the terms of the RFP;

    c. We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice, as defined in the RFP document, in respect of any Bid or request for bid issued by or any agreement entered into with Purchaser or any other public sector enterprise or any government, Central or State; and

    d. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice.

6. We understand that you may cancel the selection process at any time and that you are neither bound to accept any Bid that you may receive nor to select the Managed Service Provider , without incurring any liability to the Bidders.

7. We certify that in regard to matters other than security and integrity of the country, we or any of our affiliates have not been convicted by a court of law or indicted or adverse orders passed by a regulatory authority which would cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.

8. We further certify that in regard to matters relating to security and integrity of the country, we have not been convicted by a court of law for any offence committed by us or by any of our affiliates. We further certify that we have not been blacklisted/ suspended and have not been under a declaration of ineligibility for corrupt or fraudulent practices by GeM **OR** Department of Expenditure as on the date of submission of bid.

9. We agree and understand that the bid is subject to the provisions of the RFP document. In no case, shall we have any claim or right of whatsoever nature if the Project is not awarded to us or our bid is not opened or summarily rejected.

10. The Fee, Technical and Financial Bid are being submitted in separate covers. This Pre-Qualification read with the Technical Bid Financial Bid shall be binding on us.

11. We agree and undertake to abide by all the terms and conditions of the RFP Document. We would hold the terms of our bid valid for the number of days as stipulated in the RFP

document.

We remain, Yours sincerely,

Authorized Signature *[In full and initials]*:

Name and Title of Signatory:
Name of Firm:
Address:
Telephone:
Fax:

(Name and seal of the Bidder/Member in Charge)

4.3.2 Profile of the Bidding Firms

To be filled separately by Bidder / Lead Bidder, Consortium Partner (if any) & Subcontractor(s) (if any)

A. Background Information			
Name of the firm:			
Role:			
Year of Establishment			
Incorporated in India (Yes / No)			
Registered Office Address:			
Name and details of the CEO:			
Name of the contact person (Note: Authorized Signatory) and contact details (Email & Mobile number)			
Brief description of the Organization			
B. Financial Information (last three years)			
Financial Year	Audited Annual Turnover – Overall (INR Crores)	Audited Annual turnover for services / categories defined in Volume 2 Section 2.2 of this RFP, as appliable, (INR Crores)	
C. Other Information			
No of years of Operation in India			
Total number of Employees			
Total number of Employees in India			
List of Quality Certifications			
List of Indian Customers to whom the Firm has provided similar services in India in the last 3 (Three) years. *(Note: Similar Services refer to services / categories in Volume 2 Section 2.2 of this RFP)*			

Table 11: Profile of the Bidding Firms

4.3.3 Pre-Qualification Citations

To be filled separately by Bidder / Lead Bidder, Consortium Partner (if any) & Subcontractor(s) (if any)

S. No.	Item	Bidder's Response
1.	Name of Bidder entity	
2.	Assignment Name	
3.	Name of Client	
4.	Country	
5.	Client Contact Details *(Contact Name, Address, Telephone Number)*	
6.	Approximate Total Contract Value (TCV)	
7.	Duration of Assignment (months)	
8.	Award Date (month/year)	
9.	Completion Date (month/year)	
10.	Narrative description of the project	
11.	Details of Work that defines the scope relevant to the requirement	
12.	Documentary evidence provided/attached	

Table 12: Pre-Qualification Citations

4.3.4 Self-certificate for non-blacklisting clause

We confirm that our Company, *<Name>,* as of the date of submission of the bid is not blacklisted/ suspended by GeM as well as Department of Expenditure in India for corrupt, fraudulent or any other unethical business practices.

Sincerely,

Name & Designation of the Authorized Signatory

4.3.5 No Deviation Certificate

This is to certify that our offer is exactly in line with your tender enquiry / RFP (including amendments) no. ***<RFP number>*** dated ***<Date of RFP>***. This is to expressly certify that our offer contains no deviation on Technical (including but not limited to Scope of Work, Business Requirements Specification, Functional Requirements Specification, Cloud Requirements Specification and Technical Requirements Specification), legal or Commercial aspects in either direct or indirect form.

We understand that if any kind of deviation is found out by the Purchaser at any later stage, then the Purchaser shall have the right to take any appropriate action as deemed fit including termination of the contract.

(Authorized Signatory) Signature:

Name:

Designation:

Address:

Seal:

Date:

4.3.6 Total Responsibility

This is to certify that I, ***<Name>***, undertake the total responsibility for the defect-free operation of the proposed solution as per the requirement of the RFP for the duration mentioned in all the volumes of the RFP.

(Authorized Signatory) Signature:

Name:

Designation:

Address:

Seal:

Date:

4.3.7   Template for Integrity Pact

<div align="center">

Integrity Pact

</div>

This Integrity Pact is entered into by and between

The President of India, acting through the GeM, having its office located 3rd Floor, Tower II, Jeevan Bharti Building, Connaught Place, New Delhi - 110 001 (herein after referred to as the "Purchaser", which expression shall unless excluded by or repugnant to the context, deemed to include its successor/s in office or assign) of the First Part;

AND

<*>**, a Company incorporated under the Companies Act, 1956, having its registered office at **<***>** (hereinafter referred to as "Bidder" or "Contractor" which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the Second Part.

<div align="center">

Preamble

</div>

The Purchaser intends to award, under laid down organizational procedures, contract for Design, Development, Implementation, Operation & Maintenance of Government e- Marketplace (GeM) through an open tender process and has issued RFP bearing number **<RFP Number>.** The Purchaser values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and/or Vendor(s) Contractor(s).

To achieve these goals, the Purchaser wishes to enter into this Integrity Pact with the Bidder(s) for this tender process and execution of the Agreement and will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the Agreement for compliance with the principles mentioned above.

Section 1- Commitments of the Purchaser

1. The Purchaser commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the Purchaser, personally or through family members, will in connection with the RFP for, or the execution of the Agreement, demand, take promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Purchaser will during this tender process treat all Bidder(s) with equity and reason. The Purchaser will in particular, before and during this tender process, provide to all Bidders the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to this tender process or the Agreement execution.

c. The Purchaser will exclude from the process all known prejudiced persons.

2. If the Purchaser obtains information on the conduct of any of its officers or employees which is a criminal offence under the Indian Penal Code 1860 and/or Prevention of Corruption Act 1988, or if there be a substantive suspicion in this regard, the Purchaser will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder

1. The Bidder commits to take all measures necessary to prevent corruption. It commits itself to observe the following principles during its participation in this tender process and during the Agreement execution.

   a. The Bidder will not, directly or through any other person or firm, offer promise or give to any of the Purchaser's employees involved in this tender process or the execution of the Agreement or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during this tender process or during the execution of the Agreement.

   b. The Bidder will not enter with other bidder(s) into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in this tender process.

   c. The Bidder will not commit any offence under the Indian Penal Code 1860 and or Prevention of Corruption Act 1988; further the Bidder will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Purchaser as part of the business relationship, regarding

plans, technical bids, and business details, including information contained or transmitted electronically.

d. The Bidder of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any. Similarly, the Bidder of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder. Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative must be in Indian Rupees only. Copy of the "Guidelines on Indian agents of Foreign suppliers" is placed ahead.

e. The Bidder will, when presenting its bid, disclose all payments it has made, is committed to, or intends to make to agents, brokers, or any other intermediaries in connection with this tendering process or the award of Agreement under this tendering process.

f. The Bidder who has signed the Integrity Pact shall not approach Courts while representing the matter to IEMs and shall wait for their decision in the matter.

2. The Bidder will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from tender process and exclusion from future Contracts

If the Bidder, during the tender process or before award or during execution of the Agreement has committed a transgression through a violation of Section 2 above, or in any other form, such as to put his reliability or credibility in question, the Purchaser is entitled to disqualify the Bidder from this tender process or decide not to award the work or terminate the awarded Agreement or blacklist the Bidder.

Section 4: Compensation for Damages

1. If the Purchaser has disqualified the Bidder from this tender process prior to the award according to Section 3, the Purchaser is entitled to forfeit the Earnest Money Deposit/Bid Security deposited by the Bidder.

2. If the Purchaser has terminated the Agreement according to Section 3, or if the Purchaser is entitled to terminate the Agreement according to Section 3, the Purchaser shall be entitled to demand and recover from the Bidder Vendor the amount equivalent to Security Deposit Performance Bank Guarantee in addition to any other penalties/recoveries as per terms and conditions of the Agreement.

Section 5: Previous Transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other Central Government State Government or Central PSU entity in India or any entity in any other country conforming to the anti-corruption approach that could justify Bidder's exclusion from this tender process.

2. If the Bidder makes incorrect statement on this subject or hides any material information, the Purchaser is entitled to disqualify the Bidder from this tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings"

Section 6: Equal treatment of all Bidders

1. In case of subcontracting, the Lead contractor shall take the responsibility of the adoption of Integrity Pact by the sub-contractors.

2. The Purchaser will enter into individual Integrity Pacts with identical conditions as this one with all sub-contractors of the Vendor.

3. The Purchaser will disqualify from the process all Bidder who do sign this Integrity Pact or violate any of its provisions.

Section 7: Criminal charges against violation Bidder/Subcontractor(s)

If the Purchaser obtains knowledge of conduct of the Bidder or its Subcontractor, or of an employee or a representative or an associate of the Bidder or Subcontractor which constitutes corruption, or if the Purchaser has substantive suspicion in this regard, the Purchaser will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor/Monitors

1. The Purchaser appoints _____ as Independent External Monitor for this Integrity Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the Parties comply with the obligations under this Integrity Pact.

2. The Monitor is not subject to instructions by the representatives of the Parties and performs his functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required/ It will be obligatory for him/her to treat the information and documents of the bidders as confidential. The Monitor shall report to GeM.

3. The Bidder accepts that the Monitor has the right to access without restriction to all project documentation of the Purchaser including that provided by the Bidder. The Bidder will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors of the Vendor.

4. The Monitor is under contractual obligation to treat the information and documents of the Bidder/Subcontractor(s) of Vendor with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. In case of any conflict arising at a later date, the IEM shall inform GeM and recuse himself from that case.

5. The Purchaser will provide to the Monitor sufficient information about all meetings among the parties related to the tender process or the execution of the Agreement provided such meetings could have an impact on the contractual relations between the Purchaser and the successful Bidder. The Parties offer to the Monitor the option to participate in such meetings.

6. As soon as the Monitor notices, or believes to notice, a violation of this Integrity Pact, he will so inform the Purchaser and request the Purchaser to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action, or tolerate action.

7. The Monitor will submit a written report to the Purchaser within 8 (Eight) to 10 (Ten) weeks from the date of reference or intimation to him by the Purchaser and, should the occasion arise, submit bids for correcting problematic situations.

8. If the Monitor has reported to the Purchaser, a substantiated suspicion of an offence under relevant Indian Penal Code 1860 and Prevention of Corruption Act 1988, and the Purchaser has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner, Government of India.

    a. The word 'Monitor' would include both singular and plural.

Section 9– Pact Duration

1. This Integrity Pact begins when both Parties have legally signed it. It expires for the successful Bidder 12 (Twelve) months after the last payment under the Agreement, and for all other bidders, 6 (Six) months after the execution of the Agreement with the Vendor.

2. If any claim is made/lodged during this time, the same shall be binding and continue to be

valid despite the lapse of this pact as specified above, unless it is discharged/determined by the Purchaser.

Section 10 – Other provisions

1. This agreement is subject to Indian Law, place of performance and jurisdiction is the Office of the Purchaser first above written, i.e., New Delhi.

2. Changes and supplements of this Integrity Pact as well as termination notices need to be made in writing. Parties acknowledge that side agreements have not been made.

3. Should one or several provisions of this Integrity Pact turn out to be invalid, the remainder of this Integrity Pact remains valid. In this case, the Parties will strive to come to an agreement to their original intentions.

4. Issues like Warranty/ Guarantee etc. shall be outside the purview of IEMs

5. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

For & On Behalf of the Purchaser   **For & On Behalf of the Bidder**
(Official Seal)   **(Official Seal)**

Place: **Place:**

Date: **Date:**

Witness: Witness:

(Name & Address):   (Name & Address):

4.3.8 Cloud Service Provider's Authorization Form

(This form must be provided by the Cloud Service Provider (CSP) of the solution proposed)

No.   Date:

To

Subject: Authorization for Cloud Services for GeM

Sir,

This is to certify that we, ***<Insert the complete legal name of the CSP>***, are the Cloud Service Provider and our legal entity is registered in India. We comply with all the Pre-Qualification requirements specified in this RFP for Cloud Service Provider (CSP). We are empaneled by MeiTY for providing Government Community Cloud / Virtual Private Cloud (as applicable).

I confirm that we have signed a contract with ***<Insert the complete legal name of MSP>*** (MSP) for providing Cloud Services for GeM Solution and we comply with all the Cloud Services requirements mentioned in Volume 1 Section 3.1.4 and 8.3 of this RFP document.

I also confirm that the MSP has due authorization from us to use our Cloud Services for the purposes of hosting and running the Government eMarketplace (GeM), as per the specifications mentioned in this RFP. The MSP has authorization for use of the following set of Services (as given in below table) which are available with us, and which have been sub-contracted to the MSP:

S. No.	Authorized Services for GeM
1.	
2.	
3.	

Table 13: Authorized services for GeM

It is confirmed that even when the Purchaser changes the MSP, our Services would remain available for GeM subject to applicable SLAs and service policies for the GeM.

We hereby confirm that this undertaking is made in good faith and the aforesaid declarations are binding on us under the aforementioned Bid

For and on behalf of *<Insert CSP's company name>*

<Signed and sealed>

<Name of Authorized Signatory>

<Designation>

<Contact Details>

Cc: MSP's corporate legal name & Address

Note: The bidder in its Bid should include this CSP Authorization Form (CSPAF). This CSPAF should be on the letterhead of the CSP and should be signed by a duly authorized person of CSP. Documents in favour of authorization of the authorized person of CSP should also be submitted along with the CSPAF. The CSPAF needs to be mandatorily submitted in the format as specified, and no non-Conformity of the same shall be accepted by the Purchaser.

4.3.9 Format for Power of Attorney – Signing of Bid

POWER OF ATTORNEY

(To be on non-judicial stamp paper of Rs. 100)

Know all men by these present, we (name and address of the registered office of the Lead Bidder/ Member) do hereby constitute, appoint and authorize Mr. / Ms._____ R/o ____(name and address of residence) who is presently employed with us and holding the position of _____ as our authorized representative, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to the bid of the consortium consisting of, __ and _____ (please state the name and address of the members of the consortium) for "_____" (please state tender/bid number and details) (the "RFP"), including signing and submission of all documents and providing information / responses to Government e-Marketplace ("GeM"), representing us in all matters in connection with our bid for the said RFP.

We hereby agree to ratify all acts, deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all acts, deeds, and things done by our aforesaid attorney shall always be deemed to have been done by us.
This Power of Attorney shall be effective, binding, and operative till _____, if not revoked earlier or as long as the said Attorney is in the service of the Company, whichever is earlier.
(Name, Title and Address of the authorized representative)

For (Signature)

Accept (Signature)

Notes

1. The mode of execution of the power of attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s).

2. In the event, power of attorney has been executed outside India, the same needs to be duly notarized by a notary public of the jurisdiction where it is executed.

3. Also, wherever required, the executant(s) should submit for verification the extract of the

charter documents and documents such as a Board resolution / power of attorney, in favor of the person executing this power of attorney for delegation of power hereunder on behalf of the executant(s).

4.3.10 Format for Power of Attorney – Lead Bidder/ Member of Consortium

POWER OF ATTORNEY FOR LEAD BIDDER/ MEMBER OF CONSORTIUM

(To be on non-judicial stamp paper of Rs. 100)

Whereas the _____ (the "Purchaser") has invited bids for the _____ Project (the "Project").

Whereas, _____, _____ and _____ (collectively the "Consortium") being Members of the Consortium are interested in bidding for the Project in accordance with the terms and conditions of the Request for Proposal and other connected documents in respect of the Project, and

Whereas, it is necessary for the Members of the Consortium to designate one of them as the Lead Bidder/ Member with all necessary power and authority to do for and on behalf of the Consortium, all acts, deeds and things as may be necessary in connection with the Consortium's bid for the Project and its execution.

NOW THEREFORE KNOW ALL MEN BY THESE PRESENTS

We, _____ having our registered office at _____, M/s._____, having our registered office at _____, and M/s._____, having our registered office at_____ (hereinafter collectively referred to as the "Principals") do hereby irrevocably designate, nominate, constitute, appoint and authorise M/s _____, having its registered office at _____, being one of the Members of the Consortium, as the Lead Bidder/ Member and true and lawful attorney of the Consortium (hereinafter referred to as the "Attorney") and hereby irrevocably authorise the Attorney (with power to sub-delegate) to conduct all business for and on behalf of the Consortium and any one of us during the bidding process and, in the event the Consortium is awarded the Contract, during the execution of the Project, and in this regard, to do on our behalf and on behalf of the Consortium, all or any of such acts, deeds or things as are necessary or required or incidental to the submission of its bid for the Project, including but not limited to signing and submission of all applications, bids and other documents and writings, accept the Letter of Award, participate in bidders' and other conferences, respond to queries, submit information/ documents, sign and execute contracts and undertakings consequent to acceptance of the bid of the Consortium and generally to represent the Consortium in all its dealings with the Purchaser, and/ or any other Government Agency or any person, in all matters in connection with or relating to or arising out of the Consortium's bid for the Project and/ or upon award thereof till the Agreement is entered into with the Purchaser.

AND hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us/ Consortium.

IN WITNESS WHEREOF WE THE PRINCIPALS ABOVE NAMED HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS _____ DAY OF _____, 20___

For _____

(Signature, Name & Title)

For _____

(Signature, Name & Title)

For _____

(Signature, Name & Title)

(Executants)
(To be executed by all the Members of the Consortium)

Witnesses:

1.

2.

Notes:

1. The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required, the same should be under common seal affixed in accordance with the required procedure.

2. Wherever required, the Bidder should submit for verification the extract of the charter documents and documents such as a board or shareholders resolution/ power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Bidder.

3. For a Power of Attorney executed and issued overseas, the document will also have to be legalised by the Indian Embassy and notarised in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Bidders from countries that have signed the Hague Legislation Convention 1961 are not required to be legalised by the Indian Embassy if it carries a conforming Apostille certificate.

4.4 Annexure-4: Formats for Submission of the Technical Bid

4.4.1   Technical Bid Covering Letter

<Location, Date>

Government e-Marketplace,
3rd floor Jeevan Bharti Building, Sansad Marg
New Delhi-110001
RFP dated *[date]* for selection for Managed Service Provider

Sir,

With reference to your RFP Document dated ***<date>***, we, the undersigned, having examined all relevant documents and understood their contents, offer to provide Design, Development, Implementation, Operation & Maintenance services for Government e-Marketplace (GeM) with reference to your Request for Bid dated ***<insert date>*** and our Bid. We are hereby submitting our Pre-qualification and Technical bid for selection as Managed Service Provider. We are submitting our Bid as ***<name of the bidder>***. The Bid is unconditional and unqualified.

We hereby declare that all the information and statements made in Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification. If negotiations are held during the period of validity of the Bid, we undertake to negotiate in accordance with the RFP. Our Bid is binding upon us in accordance with the RFP.

We understand that you are not bound to accept any Bid you receive. Further:

1. We acknowledge that Purchaser will be relying on the information provided in the Bid and the documents accompanying the Bid for selection of the Managed Service Provider, and we certify that all information provided in the Bid and in the supporting documents is true and correct, nothing has been omitted which renders such information misleading; and all documents accompanying such Bid are true copies of their respective originals.

2. This statement is made for the purpose of appointment as the Managed Service Provider for the aforesaid Project.

3. We shall make available to Purchaser any additional information it may deem necessary or require for supplementing or authenticating the Bid.

4. We acknowledge the right of Purchaser to summarily reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any

account whatsoever.

5. We declare that:

   b. We have examined and have no reservations to the RFP, including any Addendum issued by the Purchaser;

   c. We do not have any conflict of interest in accordance with the terms of the RFP;

   d. We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice, as defined in the RFP document, in respect of any Bid or request for bid issued by or any agreement entered into with Purchaser or any other public sector enterprise or any government, Central or State; and

   e. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice.

6. We understand that you may cancel the selection process at any time and that you are neither bound to accept any Bid that you may receive nor to select the Managed Service Provider , without incurring any liability to the Bidders.

7. We certify that in regard to matters other than security and integrity of the country, we or any of our affiliates have not been convicted by a court of law or indicted or adverse orders passed by a regulatory authority which would cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.

8. We further certify that in regard to matters relating to security and integrity of the country, we have not been convicted by a court of law for any offence committed by us or by any of our affiliates. We further certify that we have not been blacklisted/ suspended and have not been under a declaration of ineligibility for corrupt or fraudulent practices by GeM **OR** Department of Expenditure as on the date of submission of bid.

9. We agree and understand that the bid is subject to the provisions of the RFP document. In no case, shall we have any claim or right of whatsoever nature if the Project is not awarded to us or our bid is not opened or summarily rejected.

10. The Fee, Pre-qualification and Financial Bid are being submitted in separate covers. This Technical bid read with the Pre-qualification and Financial Bid shall be binding on us.

11. We agree and undertake to abide by all the terms and conditions of the RFP Document. We would hold the terms of our bid valid for the number of days as stipulated in the RFP

document.

We remain, Yours sincerely,

Authorized Signature *[In full and initials]*:

Name and Title of Signatory:
Name of Firm:
Address:
Telephone:
Fax:

(Name and seal of the Bidder/Member in Charge)

4.4.2   Bidder's Experience - Client Citations

To be filled separately by Bidder / Lead Bidder, Consortium Partner (if any) & Subcontractor(s) (if any)

S. No.	Item	Bidder's Response
1.	Name of Bidder entity	
2.	Nature of Association *(Bidder, or Lead Bidder/ Consortium Partner in case of consortium)*	
3.	Assignment Name	
4.	Name of Client	
5.	Country	
6.	Contact Details *(Contact Name, Address, Telephone Number)*	

7.	Approximate Total Contract Value (TCV)	
8.	Duration of Assignment (months)	
9.	Award Date (month/year)	
10.	Completion Date (month/year)	
11.	Narrative description of the project	
12.	Details of Work that defines the scope relevant to the requirement	
13.	Documentary Evidence attached	
14.	Details of the proposed resources who were part of the project (if any) along with their roles. If none, mention N/A	

Table 14: Bidder's Experience - Client Citations

4.4.3 Technical Presentation and Proposed Solution

Submit a technical presentation (PDF) with focus on topics captured in Volume 2 Section 2.3.2 of this RFP. All parameters defined as evaluation criteria should be mandatorily covered.

4.4.4   Sizing Approach and Details

Refer Volume-1 Section 8.4of this RFP for minimum volumetric estimates

#	Item	Environment (Dev/UAT/ Training/ Production)	Layer (Web/ App/DB)	Total Cores	Total RAM	Storage (in TB)	OS	Virtualization software supported	Software/ Middleware Details	Sizing Considerations
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										

Table 15: Sizing Approach and Details

4.4.5 Project Plan

S. No.	Activity	Months												
		1	2	3	4	5	6	7	8	9	10	11	12
1.														
2.														
3.														
4.														

#	Role	Name	Implementation Period (Months)											Operation & Maintenance						Total person-month proposed	Distribution of Total
			1	2	3	4	5	6	7	8	9	10	...	Year 1	Year 2	Year 3	Year 4	Year 5	...	Total	Onsite

Table 16: Project Plan

4.4.6 Curriculum Vitae (CV) of Team Members

S. No.	Item	Bidder's Response		
1.	**Name of the Resource**			
2.	**Specify role to be played in the project** *(basis Volume 2 Section 2.3.3)*			
3.	**Name of Employer**			
4.	**No. of years with Current Employer**			
5.	**Total Experience (in Years)**			
6.	**Overall Experience information** *(Provide details regarding name of organizations worked for, Designation, responsibilities, tenure etc.)*			
	Name of Employer	**From**	**To**	**Designation/ Responsibilities**
6.1.				
6.2.				
7.	**Summarized professional experience** *(Relevant to the Current Project)* **in reverse chronological order**			
	From	**To**	**Company Project Position Relevant Functional, Technical and Managerial experience**	
7.1.				
7.2.				
8.	**Educational Background, Training Certification including institutions, % of marks, specialization areas etc.**			
	Degree	**Year of Award of Degree**	**University**	**% of marks**
8.1.				
8.2.				
9.	**Declaration: I hereby declare that the information provided by me in this CV is true, correct, and absolute to the best of my knowledge.**			
	Signature of the Resource:			

Table 17: Curriculum Vitae (CV) of Team Members

4.4.7 Bill of Quantities (BoQ)

Note: Per unit description & Quantities, as mentioned BoQs are to evaluate the completeness of the Technical Bid and to be used for evaluation of Technical Bid

4.4.7.1 Solution Proposed

#	Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development)	Nomenclature of Product	Version & Year of Release (if applicable)	OEM (if applicable)	Features & Functionalities	Reference in the Submitted Bid (Please provide page number/ section number/ volume)

Table 18: Bill of Quantities (BoQ)

4.4.7.2 Technology Components used for Technology Architecture by MSP for GeM Solution

#	Item Description	Reference to Volume 1 Section 8.2 Technology Architecture	Ref. to specification in Technical Bid of Bidder (Name of the Component, version, model, OEM, and other details)	Unit License policy, where applicable	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained
1.	Components used for Technical Architecture						
1.1							
..	..						
2.	Development Environment						
2.1							
3.	Testing Environment						
3.1							
..	..						
4.	Benchmarking Environment						
4.1							
..	..						

#	Item Description	Reference to Volume 1 Section 8.2 Technology Architecture	Ref. to specification in Technical Bid of Bidder (Name of the Component, version, model, OEM, and other details)	Unit License policy, where applicable	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained
5	Staging Environment						
5.1							
6.	Project Management Tools						
6.1	No of licenses						
6.2	Team members positioned for implementation						
7.	SLA Monitoring & Management Tools						
7.1	Cost of licenses						
7.2	Team members positioned for implementation						

#	Item Description	Reference to Volume 1 Section 8.2 Technology Architecture	Ref. to specification in Technical Bid of Bidder (Name of the Component, version, model, OEM, and other details)	Unit License policy, where applicable	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained
8.	Helpdesk and Technical support tool						
8.1	No of licenses						
8.2	Team members positioned for implementation						
9.	CRM Solution						
9.1	No of licenses						
9.2	Team members positioned for implementation						
10.	End to end Procurement Solution – pretender solution						

#	Item Description	Reference to Volume 1 Section 8.2 Technology Architecture	Ref. to specification in Technical Bid of Bidder (Name of the Component, version, model, OEM, and other details)	Unit License policy, where applicable	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained
10.1	No of licenses						
10.2	Team members positioned for implementation						
11.	End to end Procurement Solution –Tender preparation and publication Tender evaluation and award of contract, Post tender						
11.1	No of licenses						
11.2	Team members positioned for implementation						
12	End to end Procurement Solution –Tender						

#	Item Description	Reference to Volume 1 Section 8.2 Technology Architecture	Ref. to specification in Technical Bid of Bidder (Name of the Component, version, model, OEM, and other details)	Unit License policy, where applicable	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained
	evaluation and award of contract, Post tender						
12.1	No of licenses						
12.2	Team members positioned for implementation						
12	End to end Procurement Solution –Post tender execution monitoring						
12.1	No of licenses						
12.2	Team members positioned for implementation						

Table 19: Proposed Technology Components for GeM Solution

4.4.7.3 Other Software/ Products Proposed

#	Item	Proposed software product (Provide the Product Name and Part Number – to be filled for all COTS/open source and system software)	Whether COTS / OSS	Unit of Measurement	Number of Licenses (Development Environment)	Number of Licenses (UAT)	Number of Licenses (Data Centre/ Production)	Number of Licenses (DR Site)

Table 20: Proposed Other Components for GeM Solution

Bidder must provide the licensing matrix for all products proposed to be deployed on the Project.

4.4.7.4 Virtual Machine (VM) Compute on Cloud used for Technology Architecture by MSP for GeM Solution

#	Item Description	No of Cores per Unit of Virtual Machines	RAM per unit (In GB)	Storage per unit (in GB)	No of VM units proposed for Implementation Phase	No of VM units proposed for Benchmarking	No of VM units proposed for Operation & Maintenance Phase
1	Virtual Machines at CSP Data Centre						
2	Virtual Machines at CSP DR site						

Table 21: Proposed VM Compute on Cloud for GeM Solution

4.4.7.5   Manpower for Managed Services

Refer Volume-1 Section 8.5.1 of this RFP for minimum manpower requirements

S. No.	Profile/ Position	Number of positions as per RFP	Number of positions proposed	Proposed Effort (In man-months)

Table 22: Proposed Manpower for GeM Solution

Kindly note that Manpower proposed to be deployed by the MSP should adhere to minimum manpower requirements prescribed in Volume 1 Section 8.5 of this RFP. In case the proposed manpower requirement for any type of resource is less than the minimum number prescribed in this RFP, it will lead to summarily rejection of the bid. The team and resources working on design, development and deployment of change requests shall be separate from the resources deployed under the original Scope of Work as per this RFP.

4.4.7.6   Contact Centre & Technical Helpdesk

#	Item Description	No of proposed seats/ support engineers Go-Live
1	Contact Centre	
2	Technical Helpdesk	
..	..	
..	<< Add more rows as applicable>>	

Table 23: Proposed Business Operations Manpower for GeM solution

4.4.7.7 Network & Connectivity

S. No.	Resource Description	Type of Bandwidth	Bandwidth Offered (In MBps)	Services Offered
1	Network Connectivity between GeM Office and CSP Data Centre			
2	Network Connectivity between CSP Data Centre and DR site			
3	Network Connectivity between GeM Office and Contact Centre			
4	Network Connectivity between GeM Office and NIC			
5	Internet bandwidth at specified GeM office			
..	..			
..	<< Add more rows as applicable>>			
Total Bandwidth of Network and Internet				

Table 24: Proposed Network Connectivity for GeM solution

4.5 Annexure-5: Formats for Submission of the Commercial Bid

4.5.1 Commercial Bid Covering Letter

To,

Subject: Submission of the Commercial bid for "*<Name of the RFP>*"

Dear Sir,

We, the undersigned, offer to provide Design, Development, Implementation, Operation & Maintenance services for Government e-Marketplace (GeM) with reference to your Request for Bid dated *<insert date>* and our Bid. Our attached Commercial Bid is for the Commercial Bid Parameter of *<<Amount in words and figures>>*.

1. **PRICE AND VALIDITY**

   a. All the prices mentioned in our bid are in accordance with the terms as specified in the RFP documents. All the prices and other terms & conditions of this Bid are valid as per the bid validity specified in the final RFP document.

   b. We hereby confirm that our prices include all taxes except Service Tax.

   c. We understand that the actual payment would be made as per the existing indirect tax rates during the time of payment.

2. **UNIT RATES**

   a. We have indicated in the relevant forms the unit rates.

3. **RFP PRICING**

   a. We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in RFP documents.

4. **QUALIFYING DATA**

a. We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information / documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

5. **BID PARAMETER**

a. We declare that our Bid Parameter Value (A) is for the entire scope of the work as specified in all the Volumes of this RFP and Annexure thereto. Our bid parameter value is mentioned in the submitted Commercial Bid.

6. **PERFORMANCE BANK GUARANTEE**

a. We hereby declare that in case the contract is awarded to us, we shall submit the PBG as specified in the Volume 2 Section 3.3 of this RFP document.

b. Our Commercial Bid shall be binding upon us subject up to the expiration of the validity period of the Bid, i.e., ***<inset date>***.

We understand you are not bound to accept any Bid you receive.

We agree to abide by all the terms and conditions of all the volumes of this RFP document.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

Yours sincerely,

(Authorized Signatory) Signature:

Name:

Designation:

Address:

Seal:

Date:

4.5.2   Commercial Bid Format

All prices are to be quoted in Indian Rupees.

4.5.2.1   Bidding Parameter Value

#	Particulars	Total Bidding Parameter *(inclusive of all taxes, levies, and duties, except Goods and Services Tax) (As per Volume 1 Section 6 of this RFP)*
1.	Bidding Parameter (A)	….
	Value (in Words)	

Table 25: Commercial Bid Format

Note:

1.   The Total Bidding Parameter Value (A) will include all taxes, levies, duties, etc. (except Goods and Services Tax)

Detailed Unit Cost of Components (for future change request /enhancement / modification purposes)

4.5.2.1.1   Key GeM Components proposed for Technology Architecture by MSP

#	Item Description (Please include solution components as per proposed solution covering the business architecture)	Name of the Component, version, model, OEM, and other details	No of Licenses proposed	Unit of measurement, where applicable	Quantity	AMC/ATC in months and years wherever obtained	Cost of Items (per License)	Unit License policy, where applicable (Use Annexure if required)
1								
2								
3								
4								
5.								
6.								
7.								
8.								

Table 26: Cost summary of Technology Components for GeM Solution

The Bidder/ Lead Bidder must provide the licensing matrix, version & OEM details, along with cost break-up for all products proposed to be deployed on the project

4.5.2.1.2   Cost of Virtual Machines (VMs) on Cloud used for Technology Architecture by MSP for GeM Solution

#	Item Description	No of Cores per unit of VM	RAM per unit of VM (in GB)	Storage per VM (In GB)	Cost per unit of VM per month (including ATS) excluding taxes	Taxes, duties, levies, etc. as applicable	Cost per unit of VM per month (including ATS)
1	Per Unit of Virtual Machines at CSP Data Centre						
2	Per Unit of Virtual Machines at CSP DR						

Table 27: Cost summary of VMs for GeM Solution

* The cost per unit of Virtual Machines (VM) on Cloud at CSP DC/ DR should include all costs including the cost of all hardware components, services, software, etc. required for successfully running the GeM System.

4.5.2.1.3   Manpower Cost for Managed Services

Refer Volume-1 Section 8.5.1 of this RFP for minimum manpower requirements

S. No.	Profile/ Position	Base Rate Per Man Per Month (B)	Taxes, duties, levies, etc. as applicable (C)	Total (D=B+C)

Table 28: Cost summary of Managed Services for GeM Solution

4.5.2.1.4   Network & Connectivity Costs

S. No.	Resource Description	Bandwidth Offered (In MBps)	Cost per 1 Mbps of Bandwidth
1	Network Connectivity between GeM Office and CSP Data Centre		
2	Network Connectivity between CSP Data Centre and DR site		
3	Network Connectivity between GeM Office and Contact Centre		
4	Internet bandwidth at specified GeM office		
..	..		
..	<< Add more rows as applicable>>		
Total Cost of Network and Internet			

Table 29: Cost summary of Network Connectivity for GeM solution

4.5.2.1.5   Contact Centre & Technical Helpdesk Costs

#	Item Description	No of proposed seats or support engineers	Cost per Seat including all licenses (Excluding taxes)	Taxes, duties, levies, etc. as applicable	Total Cost per seat or support engineers, per month (including all licenses and taxes)
1	Contact Centre				
2	Technical Helpdesk				
..	..				
..	<< Add more rows as applicable>>				

Table 30: Cost summary of Business Operations Manpower for GeM solution

4.6 Annexure-6: Template for PBG

PERFORMANCE SECURITY:

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email ID>

Whereas **<<name of the supplier and address>>** (hereinafter called "the supplier") has undertaken, in pursuance of contract no. **<Insert Contract No.>** dated. **<Date>** to provide Business services for **<<name of the assignment>>** to GeM (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract.

And whereas we, **<Name of Bank>** a banking company incorporated and having its head / registered office at **<Address of Registered Office>** and having one of its offices at **<Address of Local Office>** have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs. **<Insert Value>** (Rupees **<Insert Value in Words>** only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum, or sums within the limits of Rs. **<Insert Value>** (Rupees **<Insert Value in Words>** only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition, or modification.

We undertake to pay you money so demanded not withstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any Court or Tribunal relating thereto liability under this present Guarantee being absolute and unequivocal.

This Guarantee will not be discharged or affected or suspended due to any change in the constitution, liquidation, winding up, dissolution or insolvency of the Bank or the Bidder.

We further undertake to keep this Guarantee renewed from time to time at the request of the Bidder.

This Guarantee shall be valid until *<<Insert Date>>*

Notwithstanding anything contained herein:

1. Our liability under this bank guarantee shall not exceed Rs. *<Insert Value>* (Rupees *<Insert Value in Words>* only).

2. This bank guarantee shall be valid up to *<Insert Expiry Date>*

3. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before *<Insert Expiry Date>* failing which our liability under the guarantee will automatically cease.

GOVERNMENT OF INDIA

MINISTRY OF COMMERCE & INDUSTRY

Government e-Marketplace

3rd floor, Jeevan Bharti Building, Janpath, Connaught Place, New Delhi-110001

REQUEST FOR PROPOSAL

Selection of Managed Service Provider (MSP) for Design, Development, Implementation, Operation & Maintenance of Government e-Marketplace (GeM)

RFP Number:

GeM/Hiring_Of_MSP/2022/01

Volume-3: Legal Terms & Master Service Agreements

Contents

ACRONYMS

Abbreviation	Description
AMC	Annual Maintenance Contract
ATS	Annual Technical Support
BoD	Board of Directors
CD	Compact Disk
COTS	Commercial-off-the-Shelf
CRN	Change Request Notice
CSP	Cloud Service Provider
DC	Data Centre
DR	Disaster Recovery
EPF	Employee Provident Fund
ESIC	Employees State Insurance Company
GeM	Government e-Marketplace
GFR	General Financial Rules
GST	Goods and Services Tax
IPR	Intellectual Property Right
ISO	International Organization for Standardization
IT	Information Technology
MSP	Managed Service Provider
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
RFP	Request For Proposal
SLA	Service Level Agreement

[To be executed on stamp paper of appropriate value]

THIS MASTER SERVICES AGREEMENT ("Agreement") is made on this the <***> day of <***>2022 at New Delhi, India

BY AND BETWEEN

Government e-marketplace, having its office located at _____, New Delhi (herein after referred to as '***Purchaser/ GeM***', which expression shall unless excluded by or repugnant to the context deemed to include its successor/s in office or assign);

AND

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as '***Managed Service Provider'*** **or** '***MSP'*** **or** '***Lead Bidder'*** which expression shall, unless the context otherwise requires, include its successors, and permitted assigns);

AND

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as '***Consortium Partner'*** which expression shall, unless the context otherwise requires, include its successors, and permitted assigns).

AND (if applicable)

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as '***Consortium Partner'*** which expression shall, unless the context otherwise requires, include its successors, and permitted assigns).

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'. The MSP Lead Bidder and Consortium Partner are together referred to as Consortium.

WHEREAS:

1. The Purchaser had invited bids vide its RFP _____(hereinafter referred to as 'RFP', which term shall include all corrigendum, addendums and modifications issued by the Purchaser with reference to the RFP) for Appointment of _____for_____("Project");

2. The MSP had submitted its proposal dated_____(hereinafter referred to as the 'Proposal', which term shall include all clarifications and additional documents submitted by MSP with reference to the Proposal) for the_____;

3. The Purchaser has accepted the Proposal and has agreed to appoint the MSP for the _____and has issued a letter of award notifying the MSP of its selection as successful bidder dated_____ ('Letter of Award');

4. In consideration of the foregoing and the mutual covenants and promises contained herein and other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the Parties intend to be bound legally by the terms and conditions agreed in this Agreement, for implementation of the Project.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. Definitions and Interpretations

1.1 Definitions

Terms and expressions used in this Agreement shall have the meanings set out in Schedule I of this Agreement or as defined in other volumes of the RFP. Other terms used in this Agreement are defined where they are used and have the meanings there indicated. Unless otherwise specifically defined, those terms, acronyms and phrases in this Agreement that are utilized in the Information Technology services industry or e-commerce marketplace industry shall be interpreted in accordance with their generally understood meaning in such industry.

1.2 Interpretation

In this Agreement, unless a contrary is evident:

1. Unless otherwise specified, a reference to a clause, sub-clause or section is a reference to a clause, sub-clause or section of this Agreement including any amendments or modifications to the same from time to time;

2. Words denoting the singular include the plural and vice versa and use of any gender includes the other genders;

3. References to a 'company' shall be construed so as to include any company, corporation, or other body corporate, wherever and however incorporated or established;

4. Words denoting a person shall include an individual, corporation, company, body corporate, partnership, or a trust;

5. A reference to legislation includes legislation repealing, replacing, or amending that legislation;

6. The clause headings are for convenient reference only and do not form part of this Agreement;

7. Unless otherwise specified a reference to a clause number is a reference to all its sub-clauses;

8. Where a word or phrase is given a particular meaning, it includes the appropriate grammatical forms of that word or phrase having corresponding meanings;

9. A reference to the Agreement shall, unless the context otherwise requires, includes a reference to its Annexures, Schedules and every other document forming part of this Agreement. If a term of this Agreement requires things to be done, undertaken, or completed under the Agreement, the same, if relevant, shall, unless the context otherwise require, mean to include such things to be done, undertaken, or completed under the relevant Schedules, Annexures of this Agreement.

1.3 Documents forming part of Agreement

The following documents shall be deemed to form and be read and constructed as part of the Agreement viz.:

1. This Agreement;

2. The Letter of Award;

3. The RFP;

4. The tripartite agreement to be entered into between [Internet Service Provider] for provision of bandwidth services; and

5. The Proposal

Any corrigendum/addendum/amendment/clarification issued by the Purchaser shall form part of the present Agreement. In the event of any conflict in the existing provision of the Agreement and the corrigendum/addendum/amendment/clarification, then in such circumstances, the latter shall prevail over the former.

1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

1. As between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

2. As between the provisions of RFP and any Corrigendum issued thereafter, the provisions of the Corrigendum shall, to that extent only, prevail over the corresponding earlier provision of the RFP;

3. As between the provisions of this Agreement and the RFP and the Proposal, this Agreement shall prevail;

4. As between the provisions of the RFP and the Proposal, unless otherwise decided by the Purchaser, the RFP shall prevail; and

5. As between any value written in numerals and that in words, the value in words shall prevail.

2. Scope of Work

1. In consideration of the award of the work under the RFP to the MSP and payments to be made by the Purchaser to the MSP as hereinafter mentioned, the MSP hereby covenants with the Purchaser to accomplish the entire Scope of Work as provided in Volume 1 of the RFP and clarifications, annexures, schedules etc. thereof and to perform all obligations mentioned in all volumes of the RFP.

2. The Purchaser hereby covenants to pay the MSP in consideration of the accomplishment of Scope of Work and for performance of all obligations mentioned in the RFP, the Fees or such other sum as may become payable under the provisions of the Agreement at the times and in the manner prescribed under the Agreement.

3. Notwithstanding anything contained in this Agreement, the services for internet bandwidth connectivity will be provided by the internet service provider and payments for internet services would be made by the Purchaser directly to the internet service provider as per tripartite agreement to be entered into between the Purchaser, the MSP, and the internet service provider in the format acceptable to the Purchaser. The payment made by the Purchaser to the internet service provider shall be set off by the Purchaser from the payments to be made to the MSP.

3. Term and Duration of the Agreement

1. This Agreement shall come into force and effect on the date of signing of this Agreement/contract (hereinafter the 'Effective Date') and, unless terminated earlier in accordance with the provisions of this Agreement, shall remain in force for a period of 6 (Six) years from the Effective Date or 5 (Five) years from the date of expiry of current MSP contract i.e., 1st Jan 2024, whichever is later ('Term'). The Term is further extendable for a period of 3 (Three) calendar years at the sole discretion of the Purchaser and as per the conditions mentioned in Volume 3 Section 3 Clause (2) below.

2. The Purchaser reserves the sole right to grant any extension of the Term of this Agreement and shall notify the same in writing to the MSP, at least 6 (Six) months before the expiration of the Term. The extension shall be granted by the Purchaser for a period of 2 (two) years at one time and additional 1 (one) year the next time and on the same terms and conditions as contained in this Agreement including all amendments, addendums, clarifications etc. . The Term may be extended for a maximum overall period of 3 (Three) years only. Any extension beyond the period of 3 (Three) years period shall be on mutually agreeable terms and conditions.

4. Conditions Precedent

4.1 Payment obligations to take effect upon fulfilment of Conditions Precedent

Subject to express terms to the contrary, the rights of MSP to receive payments, and obligation of the Purchaser to make payments under this Agreement, shall take effect only upon fulfilment of all the Conditions Precedent set out in Volume 3 Section 4 Clause (2) below. Notwithstanding the foregoing, the Purchaser may, at any time in its sole discretion, waive fully or partially, in writing, any of the Conditions Precedent for the MSP provided no such waiver shall affect or impair any right, power or remedy that the Purchaser may otherwise have.

4.2 Conditions Precedent to be fulfilled

The MSP shall be required to fulfil the Conditions Precedent which are as follows:

1. Furnishing by the MSP, within 15 (Fifteen) days of the receipt of the notification of award, an unconditional, irrevocable, and continuing Bank Guarantee, from a scheduled bank in India, equivalent to 3% of the total estimated contract value as mentioned in this RFP, in a form and manner acceptable to the Purchaser, which should remain valid till 6 (Six) months after expiry of the Term of the Agreement.

2. The MSP provides an undertaking to the effect that it has entered into all relevant back-end contracts with OEMs whose products or services it has quoted in the Proposal; and

3. Furnishing of duly executed Corporate Non-Disclosure Agreement in a format specified by the Purchaser.

5. Project Management

5.1 Key performance measurement

1. The MSP shall commence the performance of its obligations under the Agreement from the Effective Date and shall proceed to carry out the Services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Agreement. The MSP shall be responsible for and shall ensure that all Services are performed in accordance with the specifications and that the MSP's Team complies with such specifications and all other standards, terms and other stipulations/conditions set out hereunder.

5.2 Commencement and progress

1. The MSP shall perform the activities / services and carry out its obligations under the Agreement with due diligence, efficiency, and economy, in accordance with generally accepted techniques and practices used in the information technology and e-commerce industry and with professional engineering and standards recognized by international professional bodies and shall observe sound management, engineering, and security practices. It shall employ appropriate advanced technology and engineering practices and safe effective equipment, machinery, material, and methods.

2. The MSP shall always act, in respect of any matter relating to this Agreement, as faithful advisors to the Purchaser and shall, at all times, support and safeguard the Purchaser's legitimate interests in any dealings with MSP's Team and third parties.

3. In providing the Services, it shall use reasonable effort to prevent any disruption to Purchaser's normal business operations.

4. The MSP shall keep all back-end contracts with all OEMs, subcontractors etc. in force and up to date to ensure provision of Services as per the RFP and to meet all the SLAs.

5. The MSP shall use all material (including, without limitation, hardware, software, documents etc.) provided by the Purchaser or any of its representative, service provider etc. ('Purchaser's Material') in accordance with the license terms of such materials to the extent such terms are notified to the MSP in writing in advance. In accordance with the audit provisions herein. The MSP will reasonably cooperate with the Purchaser in respect of any third-party audit related to MSP's use and possession of any Purchaser's Material.

5.3 Final testing and Acceptance

Except as otherwise provided in Volume 1 Section 3.1.2.8 & 3.1.2.9 of this RFP, the Project shall be governed by the mechanism of final Testing and Acceptance to be put into place by the Purchaser and the MSP as under:

1. Final testing and certification criteria will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of project development and implementation covering software, hardware and network including the processes relating to the design of solution architecture, design of systems and sub- systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to compliance with SLA metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this Agreement;

2. Final testing and certification criteria will be finalized from the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed;

3. Final testing and certification criteria will consider conducting specific tests on the software, hardware, network, security, and all other aspects;

4. Final testing and certification criteria will establish appropriate processes for notifying the MSP of any deviations from the norms, standards, or guidelines at the earliest instance after taking cognizance of the same to enable the MSP to take corrective actions.

5.4   Liquidated Damages and SLAs

The MSP shall accomplish the Scope of Work under this Agreement as per the Timelines and as per the Service Levels defined in this RFP. If the MSP fails to achieve the Timelines or the Service Levels due to reasons solely attributable to the MSP or any of its Consortium Partners or subcontractors etc., the MSP shall be liable for Liquidated Damages as mentioned in Volume 1 Section 8.6.9 of this RFP. Levying of Liquidated Damages shall not be the sole and exclusive remedy available to the Purchaser and the MSP shall not be relieved from any obligations by virtue of levying of such Liquidated Damages. Liquidated damages will be capped as mentioned in Volume 1 Section 8.6.6 of this RFP. If the Liquidated Damages for any timeline or service level exceed the cap on Liquidated Damages as mentioned in Volume 1 of the RFP, the Purchaser shall have the right to treat it as an event of default and the consequences for event of default as mentioned in this Agreement shall be applicable. Additionally, Liquidated Damages and other deductions as mentioned in Volume 1 Section 3.3.1, 3.3.3 and 7 of this RFP shall also be levied on the MSP in case of breach or default. Each of the Parties shall ensure that the range of the Services / Deliverables under the SLA shall not be varied, reduced, or increased except with the prior written agreement between the Purchaser and the MSP in accordance with the provisions of Change Control Procedure set out in this Agreement.

6. Representations

6.1 Representations of the MSP

MSP (in relation to entire scope of work) and the Consortium Partner (in relation to its scope of work) hereby represent as of the date hereof, which representations shall remain in force during the Term and extension thereto, the following:

1. It is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and other agreements and to carry out the transactions contemplated hereby;

2. It is a competent provider of a variety of Information Technology and / or e- commerce marketplace services. It has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

3. It has the power and the authority that would be required to enter into this Agreement and the requisite experience, the technical know-how and the financial wherewithal required to successfully execute the terms of this Agreement and to provide services sought by the Purchaser under this Agreement;

4. It and its team have the professional skills, personnel, infrastructure, and resources/authorizations that are necessary for providing all such services as are necessary to fulfil the scope of work stipulated in the RFP and this Agreement;

5. It shall ensure that all assets/components including but not limited to equipment, software, licenses, processes, documents, etc. installed, developed, procured, deployed, and created during the term of this Agreement are duly maintained and suitably updated, upgraded, replaced with regard to contemporary requirements;

6. It and its team shall use such assets of the Purchaser as the Purchaser may permit for the sole purpose of execution of its obligations under the terms of the RFP, Proposal, or this Agreement. It shall, however, have no claim to any right, title, lien or other interest in such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term thereof;

7. It has the financial standing and capacity to undertake the Project and obligations in accordance with the terms of this Agreement;

8. This Agreement has been duly executed by it and constitutes a legal, valid, and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding, and enforceable against it in accordance with the terms hereof

9. The execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of

Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree, or order to which it is a party or by which it or any of its properties or assets is bound or affected;

10. There are, to the best of its knowledge, no material actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may materially impair its ability to perform any of its material obligations under this Agreement;

11. It has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any adverse effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

12. It has, to the best of its knowledge, complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement;

13. To the best of its knowledge, no representation by it contained herein or in any other document furnished by it to the Purchaser or its nominated agencies in relation to the any consents contains any untrue or misleading statement of material fact or omits to state a material fact necessary to make such representation not misleading;

14. No sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of Purchaser in connection therewith.

6.2 Representations of the Purchaser

The Purchaser represents to the MSP and Consortium Partner that:

1. It has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby;

2. It has taken all necessary actions under Applicable Laws to authorize the execution, delivery, and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement

3. It has the financial standing and capacity to perform its obligations under the Agreement;

4. This Agreement has been duly executed by it and constitutes a legal, valid, and binding obligation enforceable against it in accordance with the terms hereof and its obligations

under this Agreement shall be legally valid, binding, and enforceable against it in accordance with the terms thereof;

5. The execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree, or order to which it is a party or by which it or any of its properties or assets is bound or affected;

6. It has complied with Applicable Laws in all material respects

7. Purchaser's Obligation

The obligations of the Purchaser described in this Volume 3 Section 7 are in addition to, and not in derogation of, the obligations mentioned in Volume 1 of this RFP and the two are to be read harmoniously. Without prejudice to any other undertakings or obligations of the Purchaser under this Agreement or the RFP, the Purchaser shall perform the following:

1. GeM, Ministry of Commerce & Industry, or any other entity to which this Agreement is novated by GeM, shall, on behalf of the Purchaser, act as the nodal point for implementation of the Agreement and for issuance of necessary instructions, approvals, commissioning, acceptance certificate, payment etc. to the MSP.

2. The Purchaser shall ensure that approval or disapproval is provided to the MSP (as per the timelines provided for acceptance or objections of deliverables in Volume 1 of the RFP, or where no timelines are provided, within reasonable time) as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfillment of this Agreement.

3. The Purchaser's Representative shall interface with the MSP to provide the required information, clarifications and to resolve any issues as may arise during the execution of the Agreement. The Purchaser shall provide adequate cooperation in providing details, coordinating, and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Purchaser is proper and necessary.

4. The Purchaser may provide on the MSP's request, particulars information/or documentation that may be required by the MSP for proper planning and execution of work and for providing Services covered under this Agreement and for which the MSP may have to coordinate with respective vendors.

5. The Purchaser will be responsible for making all payments due to the MSP in respect of Deliverables and Services provided by the MSP and accepted by the Purchaser in accordance with the terms of this Agreement.

6. The Purchaser agrees that all Purchaser's Material provided to the MSP by or on behalf of Purchaser for MSP's use in providing the Services will be owned by or fully licensed to the Purchaser or Purchaser's authorized representative/service provider etc. and Purchaser shall have procured the right to provide such materials to the MSP. MSP will be permitted to use such materials in accordance with the license conditions of such materials.

8. Acceptance of Deliverables and Testing

8.1 Acceptance of Deliverables

The successful completion of the Project requires the acceptance by the Purchaser of all the Deliverables prepared and delivered pursuant to the Project. The acceptance procedure described in this Volume 3 Section 8 is in addition to, and not in derogation of, the acceptance procedure provided in Volume 1 of this RFP and the two are to be read harmoniously. In event of conflict, the provisions related to acceptance of Deliverables provided in Volume 1 shall prevail. Upon completion of a Deliverable, the MSP will notify the Purchaser in writing that the Deliverable has been completed and, in the case of Deliverables constituted of Software/hardware ("Operational Deliverables"), tested and/or certified as being ready for acceptance ("Ready for Acceptance") by the Purchaser. Promptly after receiving such notice, the Purchaser will evaluate the Deliverable for acceptance in accordance with this Volume 3 Section 8 or specific provisions provided in Volume 1 of this RFP.

8.2 Acceptance Procedure

Acceptance by the Purchaser ("Acceptance") requires that the Deliverables be confirmed in writing by the Purchaser to meet applicable acceptance criteria ("Acceptance Criteria") provided in the Acceptance Test Plan which, in the case of Operational Deliverables, will include the successful completion of agreed acceptance and performance testing and will also include meeting the specifications, performance standards, functional requirements and any other aspects as set out in Volume 1 of this RFP. The MSP shall prepare and propose the test procedures, which shall be described in the Acceptance Test Plan for each Deliverable and shall be subject to agreement by the Purchaser. While designing the Acceptance Test Plan, the requirements as mentioned in Volume 1 of this RFP need to be adhered to. The Acceptance tests and Acceptance Test Plan shall be sufficiently broad in scope and rigorous so as to verify that all Deliverables meet all applicable specifications, Acceptance Criteria, and performance requirements, including assurance that the Deliverables meet such tests of operational integrity as may be reasonably required by the Purchaser.

Acceptance procedures for Written Deliverables (which are all Deliverables other than Operational Deliverables) and Operational Deliverables are as follows:

1. Written Deliverables:

The MSP may submit interim drafts of written Deliverables (e.g., designs and documentation) to the Purchaser for review. The Purchaser agrees to review each interim draft within a reasonable period of time after receiving it from the MSP. When the MSP delivers a final written Deliverable to the Purchaser, the Purchaser will have the opportunity to review such written Deliverable for an acceptance period of seven (7) working days (the "Acceptance Period").

The Purchaser agrees to notify the MSP in writing either stating that the applicable written Deliverable is accepted or rejected in the form delivered by the MSP or describing with reasonable particularity any defects deficiencies that must be corrected prior to acceptance of such written Deliverable.

If the Purchaser delivers to the MSP a notice of rejection/defects/deficiencies, the MSP will correct the described defects/deficiencies as quickly as possible and, in any event, within such reasonable time period specified by the Purchaser in its notice of the rejection/deficiencies. Upon receipt of a corrected written Deliverable from the MSP, the Purchaser will have a period of seven (7) working days to review the corrected written Deliverable.

2. Operational Deliverables:

   a. To the extent not already specified in the RFP or the agreed Acceptance Test Plan, prior to the date on which the MSP is scheduled to deliver each Operational Deliverable to the Purchaser, the MSP and the Purchaser will agree upon the testing procedures for the Operational Deliverable, including without limitation detailed test cases and expected results (the "Acceptance Tests"). The Acceptance Tests will be designed to determine whether the Operational Deliverable contains any defects or deficiencies. The Purchaser will have the opportunity during the Acceptance Period to evaluate and test each Operational Deliverable in accordance with the following procedures by executing the Acceptance Tests. The Acceptance Tests may be varied with mutual consent of the Parties if required.

   b. When the MSP has completed an Operational Deliverable, the MSP should deliver the Operational Deliverable to the Purchaser at the sites mentioned by the Purchaser. The MSP shall notify the Purchaser when the Operational Deliverable is ready for Acceptance. Such notice will start the Acceptance Period, which will be seven (7) working days.

   c. The Purchaser shall notify the MSP in writing stating that the Operational Deliverable is accepted/rejected in the form delivered by the MSP or describing the defects deficiencies as provided in Volume 3 Section 8.2 (2) (d) below.

   d. If the Purchaser determines that the Operational Deliverable as delivered by the MSP deviates from its approved specifications or otherwise fails to successfully complete applicable Acceptance Tests (or a defect), the Purchaser will inform the MSP in writing, describing the defect(s) in sufficient detail to allow the MSP to recreate/rectify them. The MSP will correct any defects in an Operational Deliverable as quickly as possible after receiving the Purchaser's notice of the defects and, in any event, within ten (10) days after receiving such notice (unless a different period is otherwise specified in the notice of defect sent by the Purchaser) and provide the corrected Operational Deliverable to Purchaser for re- testing within such specified period.

   e. The Purchaser will have a reasonable additional period of time after receipt of the corrected Operational Deliverable to re-test it so as to confirm its proper functioning. The MSP will correct any further defects identified by the Purchaser during the re-test as quickly as possible, but in no event, unless otherwise directed by the Purchaser, more than five (5) days after the Purchaser notifies the MSP of the further defects.

3. Correction of Defects Deficiencies in Deliverables:

    a. If the MSP is unable to correct all the defects deficiencies preventing Acceptance of a Deliverable for which MSP is responsible after a reasonable number of repeated efforts (but not more than three (3)), the Purchaser may at its election:

        i. Allow the MSP to continue its efforts to make corrections; or

        ii. Accept the Deliverable with its defects deficiencies and deduct such proportionate amounts from the MSP's fees as is mutually agreed between the Purchaser and the MSP; or

        iii. Terminate this Agreement for cause in accordance with the procedures set forth in Volume 3 Section 13 (except that the Purchaser is under no obligation to provide the MSP any further opportunity to cure) and recover its damages subject to the limitations set forth in this Agreement; or

        iv. Invoke the risk purchase clause under this Agreement.

8.3 Acceptance

The Deliverables shall be considered accepted by the Purchaser in case the Purchaser fails to intimate acceptance of the Deliverables or its objections to the MSP within a period of thirty (30) working days from the date of receipt of the Deliverable.

9. Use of Assets by the MSP

During the Term the MSP shall:

1. Take all reasonable and proper care of the entire hardware and software, network or any other Information Technology infrastructure components used for the Project and other facilities leased, owned, or operated by the MSP (for itself or for the Purchaser or on behalf of the Purchaser) exclusively in terms of ensuring their usability for the delivery of the Deliverables and Services as per this Agreement (hereinafter the "Assets");

2. Keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) as at the date the MSP takes control of and/or first uses the Assets and during the entire Term of the Agreement;

3. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets, and which are provided to the MSP should be followed by the MSP and any person who will be responsible through MSP for the use of the Assets;

4. Take such steps as may be properly recommended by the manufacturer of the Assets and notified to the MSP or as may, in the reasonable opinion of the MSP, be necessary to use the Assets in a safe manner;

5. Ensure that the Assets that are under the control of the MSP, are kept suitably housed and in conformity with the Applicable Law and terms agreed with the Purchaser;

6. Procure permission from the Purchaser or its nominated agencies and any persons duly authorized by them to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable third-party requirements;

7. Not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to the Applicable Law;

8. Use best efforts to ensure that no lien, mortgage, hypothecation, or any other charge is created over the Assets. The MSP agrees that the MSP will inform the Purchaser immediately if the MSP feels or comes to know that a charge may have been created over any of the Asset(s). In the event a charge is created over any of the Assets due to reasons solely attributable to the MSP or any of its consortium partners subcontractors etc., the Purchaser shall have the right to get the charge removed at the risk, cost, expense of the MSP and the MSP shall make good all losses, damages, costs, fees, cess, duties, etc. borne or suffered by the Purchaser due to creation of such charge and/or in removal of such charge and/or in discharging the obligations for removal of such charge

10.   Access to locations or its Nominated Agencies

10.1   Access to locations

For so long as the MSP provides services on the locations of the Purchaser or its nominated agencies, the Purchaser shall, subject to compliance by the MSP with any safety and security guidelines which may be provided by the Purchaser and notified to the MSP in writing, provide the MSP, on a non-permanent basis and to the extent necessary, with:

1. Reasonable access to the location from where services are to be performed (except such locations like the MSP's or its subcontractor's offices etc. over which the MSP has control);

2. Subject to (1) above, the purchaser shall provide reasonable workspace, to MSP's personnel, as mentioned in Volume 1 Section 3.3.1 of this RFP, along with other related support services in such locations of the Purchaser, as may be reasonably necessary for the MSP to perform its obligations hereunder.

10.2   Limitation on access to locations

Access to locations, office equipment and services shall be made available to the MSP on an "as is, where is" basis by the Purchaser as the case may be or its nominated agencies. The MSP agrees to ensure that its employees, agents, and contractors / sub- contractors shall not use the location, services and equipment referred to in the RFP for the following purposes:

1. For the transmission of any material which is defamatory, offensive, or abusive or of an obscene or menacing character; or

2. In a manner which constitutes violation of any law or a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or confidentiality); or

3. For their own purpose or for conducting their own business or for providing services to any third party.

11. Management of Project

11.1 Governance

The review and management process of this Agreement shall be carried out in accordance with a Governance Schedule that will be mutually agreed between the Parties and shall cover all the management aspects of the Project. MSP shall prepare a Governance Schedule in consultation with the Purchaser and shall be obliged to get the same approved by the Purchaser within one month from the Effective Date. The mutually agreed Governance Schedule shall form an integral part of this Agreement.

11.2 Changes

Any changes to the scope of work and consequent impact on the SLAs shall be dealt with in accordance with the provisions of Change Control Procedure set out in Volume 1 Section 8.7 of this RFP.

11.3 Security and Safety

1. The obligations mentioned herein are in addition to (and not in derogation or substitution of) the obligations related to information security (including SLAs) mentioned in the RFP.

2. The MSP shall comply with the relevant security, safety and other requirements specified in the Information Technology Act, (as amended from time to time) and rules framed thereunder and any other Applicable Law. The MSP shall also comply with the IT Security policy and practices of the Purchaser. For avoidance of doubt, it is agreed that the MSP will at least have to comply with the security policies and practices that are to be followed by MSP as service provider to any organization which is ISO 27001:2013 compliant. In the event of any change in laws/ notifications/ guidelines/ government orders (related to security and safety) or IT security policy and practices of the Purchaser, the compliance to such changed laws and policy practices by MSP shall be subject to such terms as may be agreed by the Purchaser in its sole discretion except where compliance with change in laws is applicable on the MSP in its own right as an IT service provider or irrespective of services being provided by the MSP under this Agreement.

3. The Parties shall use reasonable endeavours to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Purchaser as the case may be, or any of their nominees' 'data, facilities or the Confidential Information.

4. The MSP shall upon reasonable request by the Purchaser as the case may be, or their nominee(s) participate in regular meetings when safety and Information Technology security matters are reviewed.

5. As per the provisions of this Agreement, the MSP shall use reasonable efforts to promptly report in writing to the Purchaser or its nominated agencies, any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and Information Technology security at the facilities of the Purchaser as the case may be.

11.4   Cooperation

Except as otherwise provided elsewhere in this Agreement, each Party *("Providing Party")* to this Agreement undertakes promptly to provide the other Party *("Receiving Party")* with all such information and co-operation which the Receiving Party reasonably requests, provided that such information and co-operation:

1. Does not require material expenditure by the Providing Party to provide the same;

2. Is reasonably required by the Receiving Party in order for it to comply with its obligations under this Agreement;

3. Cannot be construed to be Confidential Information; and

4. Is capable of being provided by the Providing Party.

Further, the MSP agrees to co-operate with the consultants, contractors, stakeholders and subcontractors of the Purchaser, or any other body appointed or nominated by the Purchaser as reasonably requested in order to accomplish the purposes and objective of this Agreement. No payment in this respect will be made by the Purchaser.

12. Financial Matters

12.1 Terms of Payment

1. Purchaser shall make payments only to the MSP at the time and in the manner set out in Volume 1 Section 6 of this RFP subject always to the fulfilment by MSP and Consortium Partners of their obligations herein except for the payment required to be made to the internet service provider providing internet connectivity as per clause 2.3 above.

2. The payments which are linked to acceptance of the deliverables will be released to MSP only on satisfactory acceptance of the deliverables for each Service as per the said schedule. Each of the Services, as specified in the Scope of Work, to be rendered by the MSP under the terms of this Agreement, shall be provided in a phased manner in accordance with the instructions and requirements of the Purchaser, as notified to MSP in writing ("Phased Services"). The fee payable for Services as specified in the Purchase orders shall be paid in accordance with Volume 1 Section 6 of this RFP; provided that the Purchaser shall have the right to require phased deployment of Services and personnel required for performance of such Services, and MSP shall ensure commissioning of such Services and deployment of the required personnel in accordance with such instructions of the Purchaser.

3. The Purchaser shall not be responsible/ obligated for making any payments or any other related obligations under this Agreement to the Consortium Partner or Consortium Partner's subcontractors or MSP's subcontractor, if any (except to internet service provider). The MSP shall be fully liable and responsible for meeting all such obligations and all payments to be made to Consortium Partner or sub- contractors (if any) and any other third party engaged by the MSP in any way connected with the discharge of the MSP's obligation under the Agreement and in any manner whatsoever.

4. All payments agreed to be made by Purchaser to the MSP in accordance with the Proposal shall be inclusive of all statutory levies, duties, taxes, and other charges whenever levied / applicable including costs of maintenance, if any and Purchaser shall not be liable to pay any such levies / other charges under or in relation to this Agreement and / or the Goods and Services.

5. Notwithstanding the foregoing, Service Tax or GST (as applicable) shall be paid by the Purchaser on actuals as per applicable laws/rates. It is clarified that the Purchaser shall not be liable to reimburse GST/Service Tax (as applicable) on the amount deducted/ recovered by GeM (on account of Liquidated Damages or any other reason) from the invoice raised by the MSP. The MSP shall be liable to raise and submit appropriate credit notes for the same to GeM and relevant tax authorities.

6. In case of change in taxes under change in law, appropriate parties shall pass the benefit of the same to the other Party. In case of such change, MSP shall submit a formal request with necessary supporting documents to the Purchaser. The Purchaser shall verify these documents and if applicable and approved in writing by the Purchaser, the MSP shall incorporate such changes into subsequent regular invoice for payment.

7. Unless otherwise provided in this Agreement or as mutually agreed between the Parties,

prices, fees as mentioned in the Commercial Proposal shall remain firm and shall not be subject to any upward revision on any account whatsoever throughout the Term.

8. It is expressly agreed that the price / fees mentioned in the Proposal by the MSP shall be deemed to include all ancillary and incidental costs and charges that are necessary for accomplishment of the scope of work and obligations mentioned in the RFP and this Agreement. No invoice for extra work/charge order on account of change order should be submitted by the MSP unless the said extra work/change order has been authorized/approved by the Purchaser in writing in accordance with the clause on Change Order.

9. In the event of the Purchaser noticing at any time that any amount has been disbursed wrongly to the MSP or any other amount is due from the MSP to the Purchaser, the Purchaser may without prejudice to its rights to recover such amounts by other means, after notifying the MSP deduct such amount from any payment falling due to the MSP. The details of such recovery, if any, will be intimated to the MSP. The MSP shall receive the payment of undisputed amount under subsequent invoice for any amount that has been omitted in the previous invoice by mistake on the part of the Purchaser or the MSP.

10. All payments are subject to deductions of applicable Liquidated Damages as provided for in Volume 1 Section 8.6.9, 3.3.3 and 7 of this RFP. For the avoidance of doubt, it is expressly clarified that the Purchaser will calculate a financial sum and debit the same against the terms of payment as set out in Volume 3 Section 21 of this Agreement as a result of the failure of the MSP to meet the Timelines and/or Service Levels.

12.2 Invoicing and Settlement

1. The MSP shall submit its invoices in accordance with the following principles:

    a. Generally, and unless otherwise agreed in writing between the Parties, the MSP shall raise a provisional invoice and a final invoice as per Volume 1 Section 6 of this RFP; and

    b. Any invoice presented in accordance with this Clause shall be in a form agreed with the Purchaser.

2. The MSP alone shall raise invoices for all the payments after receiving due approval / acceptance of the Deliverables and the Services from the Purchaser or any nominated agency. Such invoices shall be correct and accurate and shall be raised in a timely manner. Notwithstanding the foregoing, internet service provider may raise invoice directly to the Purchaser as agreed by the Purchaser. Such invoices shall be correct and accurate and shall be raised in a timely manner.

3. MSP shall raise a quarterly provisional invoice, with details related to base price and taxes (including GST) separately captured within the invoice, as per Volume 1 Section 6 of this RFP with the following supporting documents:

a. Self-certified system-generated SLA report with clear calculations of Liquidated Damages as per the mechanism defined in Volume 1 Section 8.6.6 of the RFP

b. Approved resource deployment plan for the quarter and attendance records of all manpower resources deployed by the MSP

c. Self-declaration pertaining to compliance with ESIC, EPF and other labour-laws for all manpower deployed by the MSP

The Purchaser shall examine the provisional invoices and supporting documents raised by the MSP and shall approve the invoice / suggest amendments to the invoice / seek clarifications within 30 (thirty) days from receipt of provisional invoices and all supporting documents. Post this, MSP shall raise the final invoice with supporting documents mentioned herein above.

4. Subject to the satisfactory performance of the MSP under this Agreement, the Purchaser shall make all efforts to make the payment within 15 (fifteen) days from receipt of due, valid, correct, and undisputed final invoice along with supporting documents. Payments will be subject to any deductions/ liquidated damages as agreed in this Agreement.

5. Further, the MSP agrees and acknowledges that the payment shall be made by the Purchaser only after due verification of the invoices and supporting documents and MSP shall have no claim whatsoever on account of any delayed payment.

6. Notwithstanding anything contained in Volume 3 Section 12.2 Clause (3) above, the Purchaser shall be entitled to delay or withhold payment of any invoice or part of it where the Purchaser disputes such invoice or part of it provided that such dispute is bonafide. Purchaser shall inform the MSP about the dispute within 15 (Fifteen) days of receipt of invoice. The withheld amount shall be limited to that which is in dispute. A notice of such withholding shall be provided within reasonable time of receipt of the applicable invoice. The disputed withheld amount shall be settled in accordance with the escalation procedure as set out in Governance Schedule within reasonable time after notice of reference. However, the Purchaser shall release the disputed amounts as soon as reasonably possible, upon resolution of dispute. Any exercise by the Purchaser under this clause shall not entitle the MSP to delay or withhold performance of its obligations or delivery of Deliverables / Services under this Agreement.

12.3   Tax and Deductions

1. Where applicable, payments to the MSP shall be subject to the statutory deductions under Income Tax Act, GST Act and other applicable taxes, and deductions as provided for under any law, rule, or regulation. The Purchaser shall provide the MSP with the original tax receipt of any withholding taxes paid by the Purchaser or its nominated agencies on payments under this Agreement within reasonable time after payment. All costs, damages, or expenses which the Purchaser may have paid or incurred, for which under the provisions of the Agreement, the MSP is liable, the same shall be deducted by the Purchaser from any dues to the MSP. All payments to the MSP shall be made after making necessary deductions as per terms of the

Agreement, including recovery of mobilization advance, if any, and recoveries towards facilities, if any, provided by the Purchaser to the MSP on chargeable basis.

2. The MSP shall bear all personnel taxes levied or imposed on its personnel, sub- contractor's personnel, MSP's consultants etc. on account of payment received under this Agreement. The MSP shall bear all corporate taxes, levied, or imposed on the MSP on account of payments received by it from the Purchaser for the work done under this Agreement. The MSP shall bear all taxes and duties etc. levied or imposed on the MSP under the Agreement including but not limited to Customs duty, Excise duty and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof up to the date for submission of final price bid, i.e., on account of payments received by him from the Purchaser for work done under the Agreement. The MSP shall also be responsible for having his sub-contractors under its sub-contract(s) to pay all applicable taxes on account of payment received by the sub-contractors from the MSP for works done under the sub-contracts in relation to this Agreement and the Purchaser will in no case bear any responsibility for such payment of taxes. It shall be the responsibility of the MSP to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. The MSP shall also provide the Purchaser such information, as it may be required in regard to the MSP's details of payment made by the Purchaser under the Agreement for proper assessment of taxes and duties. The MSP and his sub-contractors or their personnel shall bear all the taxes if any, levied on the MSP's, sub-contractors' and the MSP's personnel. The amount of tax withheld by the Purchaser shall at all times be in accordance with Indian Tax Law and the Purchaser shall promptly furnish to the MSP original certificates (Challans) for tax deduction at source and paid to the Tax Authorities. The MSP agrees that it and its sub- contractors shall comply with the Indian Income Tax Act in force from time to time and pay Indian Income Tax, as may be imposed/levied on them by the Indian Income Tax Authorities, for the payments received by them for the works under the Agreement.

3. Should the MSP and/or Consortium Partner fail to submit returns/pay taxes in times as stipulated under the Indian Income Tax Act and consequently any interest or deductions is imposed by the Indian Income Tax authority, the MSP and/or Consortium Member, as the case may be, shall pay the same.

13. Events of Default, Termination and Suspension

13.1 Events of Default by MSP

1. The failure on the part of the MSP to perform any of its obligations or comply with any of the terms of this Agreement shall constitute an Event of Default on the part of the MSP. The events of default as mentioned above may include, inter-alia, the following:

   a. the MSP has failed to perform the obligations under this Agreement and/or any terms and conditions of this Agreement; or

   b. MSP has exceeded cap on any Liquidated Damages;

   c. the MSP or its team has failed to conform with any of the service/ technical specifications and/or legal and commercial aspects as set out in the RFP or this Agreement;

   d. the MSP has failed to demonstrate or sustain any representation or warranty made by it in this Agreement, with respect to any of the terms of its Proposal, the RFP, and this Agreement;

   e. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the MSP or Consortium Partner;

   f. The MSP or Consortium Partner or their team has failed to comply with or is in breach or contravention of any Applicable Laws;

   g. There is an undue delay in achieving the agreed timelines for delivering the services under this Agreement due to reasons solely attributable to the MSP or the Consortium Partner;

   h. Where it comes to the Purchaser's attention that the MSP or Consortium Partner (or their Team) is in a position of actual conflict of interest with the interests of the Purchaser, in relation to any of terms of the MSP's Proposal, the RFP or this Agreement;

   i. If it comes to knowledge of the Purchaser that the MSP or Consortium Partner or any of their personnel or their sub-contractors or such sub-contractor's personnel have been involved in any fraudulent or corrupt practices or any other practice of similar nature.

   j. Quality of Deliverables and services by the MSP is consistently not to the satisfaction of the Purchaser

2. Where there has been an occurrence of such Event of Defaults, inter alia, as stated above, the Purchaser shall issue a notice of default to the MSP, setting out specific defaults deviances omissions and providing a period of up to thirty (30) days to enable the MSP to remedy the

default/deviances omissions committed.

3. Where despite the issuance of a default notice to the MSP by the Purchaser the MSP fails to remedy the default to the reasonable satisfaction of the Purchaser, the Purchaser may, where it deems fit, issue to the MSP another default notice or proceed to adopt such remedies as may be available to the Purchaser including but not limited to the remedies provided in Volume 3 Section 13.2 below.

13.2   Consequences for Events of Default

Where an Event of Default subsists or remains uncured even after expiry if 30 (Thirty) days as mentioned in Volume 3 Section 13.1 (2), the Purchaser shall be entitled to:

1. Impose any such reasonable obligations and conditions and issue any clarifications as may be necessary to, inter alia, ensure smooth continuation of the Services and the project which the MSP shall be obliged to comply with. The MSP shall in addition take all available steps to minimize loss resulting from such event of default.

2. Suspend all corresponding and relevant payments to the MSP under the Agreement (except for milestones which have been successfully achieved) by written notice of suspension to the MSP provided that such notice of suspension shall (a) specify the nature of failure; and (b) request the MSP to remedy such failure within a specified period from the date of receipt of such notice of suspension by the MSP.

3. Terminate this Agreement in full or in part.

4. Invoke the Performance Bank Guarantee and other Guarantees furnished hereunder, enforce indemnity provisions, recover such other costs/losses and other amounts from the MSP which may have resulted from such default and pursue such other rights and/or remedies that may be available to the Purchaser under law.

5. Nothing herein shall affect the continued obligation of the MSP to perform all their obligations and responsibilities under the Agreement in an identical manner as were being performed before the occurrence of the default.

13.3   Termination for Breach

The Purchaser may, terminate this Agreement by giving the MSP a prior and written notice of up to 30 (Thirty) days indicating its intention to terminate where the Purchaser is of the opinion that there has been such Event of Default on the part of the MSP which has not been cured within the 30 (Thirty) days' notice period provided as per Volume 3 Section 13.1 (2). The Purchaser may, in its sole discretion, afford a further reasonable opportunity to the MSP to explain the circumstances leading to such a breach and may increase the time limit for curing such breach before terminating the Agreement.

13.4 Termination for Convenience

The Purchaser may, by written notice of 90 (Ninety) days sent to the MSP, terminate the Agreement, in whole or in part at any time for its convenience. The notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of work under the Agreement is terminated, and the date upon which such termination becomes effective. The Purchaser may, at its discretion, relax or absolve the MSP from following the timelines and/or service levels related to the part of the Agreement which is being terminated.

13.5 Effects of Termination

1. In the event of expiry of the Term or termination of this Agreement due to any cause whatsoever, the MSP and the Purchaser shall comply with the Exit Management Schedule /Plan set out as Schedule IV of this Agreement (and as revised from time to time).

2. Where the termination of the Agreement is prior to its stipulated term on account of an Event of Default on the part of the MSP, the Purchaser shall pay the MSP the amount due and payable up to the date of effective date of termination.

3. Where the termination of the Agreement is prior to its stipulated term on account of termination for convenience by the Purchaser, the Purchaser shall pay the MSP the amount due and payable up to the date of effective date of termination. For avoidance of doubt, payment applicable till the effective date of termination will be basis Volume 1 Section 6 of this RFP. The Purchaser will compensate the MSP on mutually agreed terms for reasonable and fair value of sunk in cost directly incurred by the MSP.

4. Nothing herein shall restrict the right of the Purchaser to invoke the Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the Purchaser under this Agreement and/or the Applicable Law.

5. Any and all payments under this clause shall be payable only after the MSP has complied with and completed the transition and exit management as per the Exit Management Plan to the satisfaction of the Purchaser. In case of expiry of the Agreement, the last due payment shall be payable to the MSP after the MSP has complied with and completed the transition and exit management as per the Exit Management Plan to the satisfaction of the Purchaser.

6. Without prejudice any other rights, the Purchaser may retain such amounts from the payment due and payable by the Purchaser to the MSP as may be required to offset any losses caused to the Purchaser as a result of any act/omissions of the MSP.

13.6 Rights other than Termination

1. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Agreement that are expressly or by implication intended to come into or continue in force on or after such termination.

2. The termination provisions set out in this Volume 3 Section 13 are in addition to any termination rights that the Purchaser may have under this Agreement/RFP and are in addition to, and without prejudice to, other rights that the Purchaser may have under law and this Agreement.

14. Indemnification and Limitation of Liability

14.1   General Indemnity

Subject to Volume 3 Section 14.2 below, the MSP (the "Indemnifying Party") undertakes to indemnify, hold harmless and defend the Purchaser and its nominated agencies (the "Indemnified Party") from and against all losses, claims, damages, compensation (including attorney fees) etc. on account of bodily injury, death or damage to tangible personal property arising in favour of any person, company or other entity (including the Indemnified Party) attributable to - the Indemnifying Party's gross negligence or willful default.

14.1 A Subject to Clause 14.2 below, the Indemnifying Party shall also indemnify, hold harmless and defend, Indemnified Party from and against all claims, actions, liabilities, losses, damages, and expenses (including legal expenses) incurred by the Indemnified Party, which arise, directly or indirectly, out of or in connection with the performance of the Services by the MSP including any defect, fault, deficiency in the applications/system developed and or maintained by the Indemnifying Party or any of its Consortium Partner(s) or sub- contractors etc. attributable to Indemnifying Party or any of its Consortium Partner(s) or sub-contractors etc. act or omission. It is clarified that the Indemnifying Party shall also indemnify, hold harmless and defend the Indemnified Party from all claims, actions, liabilities, losses, damages, and expenses (including legal expenses) incurred by the Indemnified Party on account of any breach, defect, default of its Consortium Partner/ sub-contractor.

14.2   IPR Indemnity

If the Indemnified Party notifies the Indemnifying Party in writing –

1. of a third-party claim against the Indemnified Party that any Goods Deliverables / Services provided by the Indemnifying Party infringes a copyright, trade secret, patent, or other intellectual property rights of any third party, or

2. of a third-party claim against the Indemnified Party or any of its service provider that any Purchaser's Material provided by the Indemnified Party or any of its service provider has been used by Indemnifying Party in breach of licensing or use terms for such Purchaser's Material, provided such licensing or use terms are notified to the Indemnifying Party in advance in writing;

the Indemnifying Party will defend such claim at its expense and will pay any costs or damages that may be finally awarded against the Indemnified Party or its service provider, provided, the Indemnifying Party will not indemnify the Indemnified Party if the claim of infringement is caused by (a) The Indemnified Party's misuse or modification of the Deliverables; (b) The Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party; (c) The Indemnified Party's use of the Deliverables in combination with any product or information not owned or developed or supplied by the Indemnifying Party (d) compliance with technical specifications, instructions of the Purchaser; (e) inclusion in the Deliverables of any content or other materials provided by Indemnified Party and the infringement relates to or arises from such

Indemnified Party materials or provided material; or (f) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided by the Indemnifying Party. If any of the Deliverables is or likely to be held as infringing, the Indemnifying Party shall at its expense and option either (i) procure the right for the Indemnified Party to continue using it, (ii) replace it with a non-infringing equivalent, or (iii) modify it to make it non-infringing.

14.3 Conditions for Indemnity

Without prejudice to the rights of the Purchaser in respect of indemnification for any claim:

1. The Purchaser shall notify the MSP upon receipt of any notice of claim setting out in reasonable particulars, the details of such notice of claim;

2. Immediately upon receipt of notification of any claim from the Purchaser, the MSP within a period of 5 (Five) days from date of receipt of such notice from the Purchaser, notify the Purchaser whether the MSP wish to assume the defense in relation to such claim (including settlement or resolution thereof). Thereafter, the MSP shall be entitled in consultation with the Purchaser, and only to the extent such action does not in any manner compromise, prejudice or adversely affect the interests of the Purchaser, to take such action as mutually agreed upon by MSP and the Purchaser to avoid, dispute, deny, resist, appeal, compromise or consent such claim, within a period of 30 (Thirty) days from the date of receipt of such claim notification;

3. Notwithstanding anything contained herein, the MSP and the Purchaser agree and covenant that a notice by the Purchaser to the MSP in relation to the claim as aforesaid shall amount to express acceptance and consent by the MSP to indemnify the Purchaser for all losses in relation to such claim. Upon notice by the MSP, the Purchaser shall reasonably co-operate with the MSP at the sole costs of the MSP, only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the Purchaser. The Purchaser shall have the right, at its option, to participate in the defense of such claim at its own cost and expense;

4. If the MSP fails to take any action as per the above clause within the time period as specified therein, the Purchaser shall have the right, in its absolute discretion, to take such action as it may deem necessary to avoid, dispute, deny, resist, appeal, compromise or contest or settle any claim (including without limitation, making claims or counterclaims against third parties). If the MSP does not assume control of the defense of such claims (as mentioned above), the entire defense, negotiation, or settlement of such claim by the Purchaser shall be deemed to have been consented to by, and shall be binding upon, MSP as fully as though the MSP alone had assumed the defense thereof and a judgement had been entered into by the MSP, for such claim in respect of the settlement or judgement.

5. **Assigned IPR** - The Purchaser shall own all Assigned IPR, and the MSP shall assign to all Assigned IPR to the Purchaser from the date of its creation, with full title guarantee and to the fullest extent possible, to hold absolutely all right, title and interest, whether legal or beneficial in and relating to all such Assigned IPR and all accrued rights of action in relation

to that Assigned IPR. Both the Purchaser and the MSP agree that all applications for registration of patents, registered designs and trademarks that include or will include Assigned IPR will vest in the Purchaser with effect from the date on which such registrations are granted.

6. **MSP IPR** - The MSP would grant to the Purchaser a perpetual, worldwide, non-exclusive, irrevocable and royalty free license to use and sub-license MSP IPR in any deliverable or materials created under or in connection with GeM Platform services (including all working notes and drafts) or delivered to GeM in connection with the GeM IPR ("GeM Services") and any MSP IPR in any Services.

7. **IPR consent:** The MSP shall not embed or use any other MSP or any third party proprietary IPR in any services without the prior written agreement of the GeM and, for the avoidance of doubt, where the Purchaser does give consent, any such intellectual property rights shall be licensed in accordance.

8. **Purchaser IPR**: The Purchaser hereby grants to the MSP for the Term a non-exclusive, revocable, and royalty-free license to use any intellectual property rights in any materials made available to the MSP as is required by the MSP to provide the Services.

9. **Confidentiality & Data**

   a. **Confidentiality:** The Purchaser, the MSP and the Consortium Partner hereby agree that all information (whether written/ tangible or oral/ intangible) furnished by the Purchaser or any third party to the MSP/ Consortium/ or its Sub-Contractor/ representatives/ employees/ agents, in connection with this Agreement, and all information/ documents/ materials prepared by MSP/ Consortium/ Sub-Contractor/or their representatives/ employees/ agents, in relation to the information obtained by the MSP in connection to and under the purview of this Agreement shall be the confidential information; and the terms of the NDA shall apply in respect of this Agreement and its subject matter provided that nothing in the non-disclosure agreement shall apply to prevent the Purchaser sharing the IPR licensed (Intellectual Property Rights) or any services with any third party.

   b. **Assignment and Subcontracting:** The MSP shall not, without prior written consent of the GeM, assign, subcontract, transfer, charge or otherwise dispose of any interest in this Agreement.

14.4   Limitation of Liability

1. The liability of the MSP (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables, Goods, Services and risk purchase clause covered by this Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed the higher of (a) value of the Performance Bank Guarantee OR (b) an amount equal to the fees received by the MSP from the Purchaser under this Agreement during the Twelve (12) months period immediately preceding the date of arising of any event of

default/incident/cause of action

2. The liability of the Purchaser (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement shall be limited to the amount of unpaid fees which is due and payable to the MSP under this Agreement at the time of arising of any event of default/incident/cause of action. It is hereby clarified that the said liability of the Purchaser shall not include any kind of deductions which the Purchaser is entitled to deduct in terms of this Agreement.

3. Except for damages arising from gross negligence and willful misconduct, in no event shall either party be liable for any consequential, incidental, indirect, special, or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) even if it has been advised of their possible existence. The limitation set out in this Clause will not apply to the liability of the MSP to the extent such liability results from MSP's breach of its confidentiality obligations.

4. Notwithstanding anything contained in the foregoing, the liability cap for the MSP given under Volume 3 Section 14.5 (1) shall not be applicable to (a) the indemnification obligations set out in this Volume 3 Section 14.1 14.2, 24.3 (5), (b) breach of confidentiality obligations, and (c) any damages arising out of gross negligence and willful misconduct of the MSP/ Consortium Partner or its sub-contractors/ employees/ agents/ consultants, etc.

14.5   Allocation of liability

The allocations of liability in Volume 3 Section 14 represent the agreed and bargained-for understanding of the parties and compensation for the Services / Deliverables reflects such allocations.

15. Force Majeure

15.1 Definition of Force Majeure

The MSP or the Purchaser, as the case may be, shall be entitled to suspend or excuse performance of its respective obligations under this Agreement to the extent that such performance is impeded by an event of force majeure ('Force Majeure').

15.2 Force Majeure Events

1. A Force Majeure event means any event or circumstance, or a combination of events and circumstances referred to in this Clause, which is beyond the reasonable control of the affected Party;

2. such Party could not have prevented or reasonably overcome with the exercise of reasonable skill and care;

3. does not result from the negligence of such Party or the failure of such Party to perform its obligations under this Agreement;

4. is of an incapacitating nature and prevents or causes a delay or impediment in performance; and

5. may be classified as all or any of the following events:

   a. act of God like earthquake, flood, inundation, landslide, storm, tempest, hurricane, cyclone, lightning, thunder, or volcanic eruption that directly and adversely affect the performance of services by the MSP under this Agreement;

   b. radioactive contamination or ionizing radiation or biological contamination (except as may be attributable to the MSP's use of radiation or radioactivity or biologically contaminating material) that directly and adversely affect the performance of services by the MSP under this Agreement;

   c. pandemics, epidemics, quarantine restrictions ,industry wide strikes, lockouts, boycotts, labour disruptions or any other industrial disturbances, as the case may be, not arising on account of the acts or omissions of the MSP and which directly and adversely affect the timely implementation and continued operation of the Project; or

   d. an act of war (whether declared or undeclared), hostilities, invasion, armed conflict or act of foreign enemy, blockade, embargo, prolonged riot, insurrection, terrorist or military action, civil commotion, or politically motivated sabotage, for a continuous period exceeding seven (7) days that directly and adversely affect the performance of services by the MSP under this Agreement.

For the avoidance of doubt, it is expressly clarified that the failure on the part of the MSP under this Agreement or the SLA to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of this Agreement or the SLA against natural disaster, fire, sabotage, or other similar occurrence shall not be deemed to be a Force Majeure event. For the avoidance of doubt, it is further clarified that any negligence in performance of Services which directly causes any breach of security like hacking shall not be considered as arising due to forces of nature and shall not qualify under the definition of "Force Majeure". The MSP will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes, and technology to prevent any breach of security and any resulting liability therefrom (wherever applicable).

It is agreed between the Parties that the provisions related to force majeure as referred above shall be applicable to the SLAs (mentioned in, inter alia, sub-section 'Systems availability SLAs' and sub-section 'Cloud Services SLAs' in Volume 1 Section 8.6.9.1.2 of this RFP) even in case where the DC and DR of the Cloud Service Provider (CSP) are not in different seismic zone. In addition, the CSP shall have to demonstrate in its technical proposal as to how it proposes to maintain the said SLAs in case of natural disaster / force majeure event.

15.3   Notification procedure for Force Majeure

1. The affected Party shall notify the other Party of a Force Majeure event within seven (7) days of occurrence of such event. If the other Party disputes the claim for relief under Force Majeure, it shall give the claiming Party written notice of such dispute within thirty (30) days of such notice. Such dispute shall be dealt with in accordance with the dispute resolution mechanism in the Agreement.

2. Upon cessation of the situation which led the Party claiming Force Majeure, the claiming Party shall within seven (7) days thereof notify the other Party in writing of the cessation and the Parties shall as soon as practicable thereafter continue performance of all obligations under this Agreement.

15.4   Allocation of costs arising out of Force Majeure

1. Upon the occurrence of any Force Majeure event prior to the Effective Date, the Parties shall bear their respective costs and no Party shall be required to pay to the other Party any costs thereof.

2. Upon occurrence of a Force Majeure event after the Effective Date, the costs incurred and attributable to such event and directly relating to the Project ('Force Majeure Costs') shall be allocated and paid as follows:

   a. Upon occurrence of an event mentioned in Volume 3 Section 15.2 (1), (2), (3) and (4), the Parties shall bear their respective Force Majeure Costs and neither Party shall be required to pay to the other Party any costs thereof.

b. Save and except as expressly provided in this Clause, neither Party shall be liable in any manner whatsoever to the other Party in respect of any loss, damage, costs, expense, claims, demands, and proceedings relating to or arising out of occurrence or existence of any Force Majeure event or exercise of any right pursuant hereof.

15.5   Consultation and duty to mitigate

Except as otherwise provided in this Clause, the affected Party shall, at its own cost, take all steps reasonably required to remedy and mitigate the effects of the Force Majeure event and restore its ability to perform its obligations under this Agreement as soon as reasonably practicable. The Parties shall consult with each other to determine the reasonable measures to be implemented to minimize the losses of each Party resulting from the Force Majeure event. The affected Party shall keep the other Party informed of its efforts to remedy the effect of the Force Majeure event and shall make reasonable efforts to mitigate such event on a continuous basis and shall provide written notice of the resumption of performance hereunder.

16. Confidentiality and Information Security

1. The Purchaser may allow the MSP to utilize highly Confidential Information including confidential public records/ personal identifiable information and the MSP shall maintain the highest level of secrecy, confidentiality, and privacy with regard to such Confidential Information. The MSP/ Consortium Partner and its Sub-contractors/ Employees/ Agents etc. shall use its best efforts to protect the confidentiality, integrity and proprietary of the Confidential Information. No member of MSP's / Consortium Partner and its Sub-contractors/ Employees/ Agents etc shall, without prior written consent from the Purchaser, disclose any information to any person (including, without limitation, any member of the media, or any other individual, corporation, partnership, limited liability company, Government agency, or group) in any manner whatsoever, and make any use of any Confidential and Proprietary Information given by the Purchaser, except for purposes of performing this Agreement. Each member of MSP's Team/ Consortium Partner/ sub-contractor/ and their employees/ agents, etc shall keep all the Confidential and Proprietary Information, provided by the Purchaser to them or their respective employees as confidential.

2. Additionally, the MSP shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management, and maintenance of the systems/facilities. The MSP shall use the information only to execute this Agreement.

3. The MSP / Consortium Partner and its sub-contractor/ employees / consultants / agents, without prior written consent of the Purchaser shall not provide consultancy or any other kind of services to any third party in relation to the Purchaser or the Purchaser's portal. The MSP shall ensure that all its sub-contractors/ employees/ and agents shall comply with the obligations set out in this clause.

4. The Purchaser shall retain all rights to prevent, stop and if required take the necessary punitive action against the MSP regarding any forbidden disclosure. The Purchaser reserves the right to adopt legal proceedings, civil or criminal, against the MSP in relation to a dispute arising out of breach of obligation by the MSP under this clause.

5. The MSP shall execute a corporate non-disclosure agreement with GeM, in the format provided by the Purchaser and shall ensure that employees, consultants, agents and sub-contractors of the MSP, as requested by the Purchaser shall execute individual/ corporate non-disclosure agreements, which have been duly approved by the Purchaser with respect to this Project.

6. The MSP should only disclose the Confidential Information in the following circumstances:

   a. with the prior written consent of the Purchaser;

   b. to a member of the MSP's Team ("Authorized Person") provided the Authorized Person needs to know the Confidential Information for accomplishment of the Services and the Authorized Person has executed a confidentiality agreement with the Purchaser prior to receiving such information (MSP and every other member of MSP's Team shall ensure that such Authorized Person to whom such

information is disclosed are bound by the similar confidentiality obligations as applicable to each member of MSP's Team. Disclosure to any such Authorized Person shall be made in confidence on need-to-know basis i.e., so far as may be necessary for such Authorized Person for the purposes of-performance of the obligations of this Agreement); and

   c. if and to the extent that the MSP is compelled legally to disclose the Confidential Information.

7. When the MSP is aware of any steps being taken or considered to compel legally the MSP or an Authorized Person to disclose the Confidential Information, it shall:

   a. to the extent legally permitted, defer, and limit the disclosure with a view to preserving the confidentiality of the Confidential Information as much as possible;

   b. promptly notify the Purchaser; and

   c. do anything reasonably required by the Purchaser to oppose or restrict that disclosure.

8. The MSP shall notify the Purchaser promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Agreement or with the authority of the Purchaser.

9. The MSP shall not carry any written material, layout, diagrams, floppy diskettes, pen-drive, CDs, hard disk, storage tapes or any other media out of the Purchaser premise without written permission from the Purchaser. The MSP's personnel shall follow the Purchaser's Information Security policy. The MSP acknowledges that the Purchaser's business data and other Purchaser proprietary information or materials, whether developed by the Purchaser or being used by the Purchaser pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to the Purchaser; and the MSP agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by the MSP to protect its own proprietary information. The MSP recognizes that the goodwill of the Purchaser depends, among other things, upon keeping such proprietary information confidential and that unauthorized disclosure of the same by the MSP could damage the Purchaser, and that by reason of the MSP's duties hereunder, the MSP may come into possession of such proprietary information, even though the MSP does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. The MSP shall use such information only for the purpose of performing the said services. The MSP shall, upon termination of this Agreement for any reason, or upon demand by the Purchaser, whichever is earliest return any and all information provided to the MSP by the Purchaser, including any copies or reproductions, both hardcopy and electronic.

10. The obligations of confidentiality under this Agreement shall remain in force for the Term of the Agreement and shall also survive the termination of this Agreement

11. Obligations under this Volume 3 Section 16 shall not apply to any information which is: (a) previously known to the MSP at the time of disclosure without obligation of confidentiality, (b) independently developed by MSP and not derived from the Confidential Information supplied by the MSP or the participation of individuals who have had access to Confidential Information, (c) in or subsequently comes into the public domain (other than as a result of a breach of this Agreement); or (d) required to be disclosed by the MSP by law, regulation, court order or other legal process, provided, where legally permissible, MSP provides written notice to the Purchaser prior to such disclosure and provide reasonable assistance to the Purchaser in retaining the confidentiality of such information.

12. The MSP undertakes not to make any press announcement or publicize the Agreement or any part thereof in any way, except with the prior written consent of the Purchaser.

Protection and Security of Personal Data

13. Where the contractor is processing Personal Data, as a Data Processor or otherwise for the Purchaser, the MSP shall:

    a. Process the Personal Data only as per instructions from the Purchaser (which may be specific instructions or instructions of a general nature) as set out in this Agreement or as otherwise notified by the Purchaser;

    b. Comply with all applicable laws;

    c. Process the Personal Data only to the extent, and in such manner as is necessary for the discharge of the contractor's obligations under this Agreement or as is required by Law or any Regulatory Body;

    d. Implement appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful Processing and accidental loss, destruction, damage, alteration, or disclosure. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful Processing, accidental loss, destruction, or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

    e. Take reasonable steps to ensure the reliability of its staff and agents who may have access to the Personal Data;

    f. Obtain prior written consent from the Authority to transfer the Personal Data to any sub-contractor for the provision of the Services;

    g. Not cause or permit the Personal Data to be transferred, stored, accessed, viewed, or processed outside of India without the prior written consent of the Purchaser.

    h. Ensure that all staff, employees, and agents required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this clause.

i. Ensure that none of the staff and agents publishes or disclose any personal data to any third parties unless directed in writing to do so by the Purchaser. Not disclose Personal Data to any third parties in any circumstances other than with the written consent of the Purchaser. or compliance with a legal obligation imposed upon the Purchaser.

13. Notify the Purchaser.(within five Working Days) if it receives; a) a request from an employee of the Purchaser to have access to his or other employees' Personal Data; or b) a complaint or request relating to the Purchaser's obligations under the law;

14. The provision of this clause shall apply during the contract/ agreement Period and indefinitely after its expiry

17. **Stipulated Time Schedule**

The Time Schedule has been mentioned in the Volume 1 of the RFP. The MSP shall perform the activities and comply in all respects with the critical dates, which will be communicated by the Purchaser to the MSP's team, as the case may be, and the parties hereby agree that failure on part of the MSP, and Consortium Partner to meet the critical dates without prejudice to any other rights that the Purchaser may have, may lead to the imposition of such obligations as are laid down in levy of Liquidated Damages as set out in the RFP and/or termination of the Agreement at the discretion of the Purchaser.

18. Audit, Access, and Reporting

1. The Purchaser reserves the right to inspect and monitor/assess the progress of the project at any time during the course of the Agreement, after providing due notice to the MSP. The Purchaser may demand and upon such demand being made, the Purchaser shall be provided with any document, data, material, or any other information which it may require, to enable it to assess the progress of the project.

2. The Purchaser shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by the MSP of its obligations/functions in accordance with the standards committed to or required by the Purchaser and the MSP undertakes to cooperate with and provide to the Purchaser/any other agency appointed by the Purchaser, all documents and other details as may be required by them for this purpose. To the extent reasonably possible, the Purchaser shall endeavour not to appoint a competitor of MSP as auditor. Any deviations or contravention, identified as a result of such audit/assessment, would need to be rectified by the MSP failing which the Purchaser may, without prejudice to any other rights that it may have issue a notice of default. Cost of acquisition of deliverables by the MSP and other sub-contractors is out of the purview of audit/inspections.

3. Without prejudice to the foregoing, the MSP shall allow access to the Purchaser or its nominated agencies to all information which is in the possession or control of the MSP, and which relates to the provision of the Services/Deliverables as set out in the Audit, Access, and Reporting Schedule and which is reasonably required by the Purchaser to comply with the terms of the Audit, Access and Reporting Schedule set out as Schedule II of this Agreement.

4. The MSP shall provide all such reports and documents as may be requested by the Purchaser for Purchaser's internal compliance purposes within 15 (Fifteen) days (or such other period allowed by the Purchaser) of receipt of request from the Purchaser.

19. Ownership and Intellectual Property Rights

All deliverables, outputs, plans, drawings, specifications, designs, reports, working papers and any other documents prepared by the MSP under this Agreement shall become and remain the property of the Purchaser and must not be shared with third parties or reproduced, whether in whole or part, without the Purchaser's prior written consent.

1. **COTS products and enhancements:** All COTS products and related solutions and fixes provided by the MSP pursuant to this Agreement shall be licensed to the Purchaser according to the terms of the license agreement packaged with or otherwise applicable to such product. Such licenses shall be brought on behalf of and in the name of the Purchaser or mentioning the Purchaser as the end user of such licenses. MSP would be responsible for arranging any licenses associated with products. "Product" means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing which are made available to the Purchaser for license which is published by product owner or its affiliates, or a third party. "Fixes" means product fixes that are either released generally (such as commercial product service packs) or that are provided when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing. Unless otherwise specifically restricted by the Licensing Terms of the COTS products, all intellectual property rights in any development / enhancement / customization etc. done on the COTS products pursuant to this Agreement shall be owned by the Purchaser. The MSP undertakes to execute all such agreements / documents and assist the Purchaser in filing all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the Purchaser. The MSP shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for use of the Deliverables, services, applications, services etc. provided by the MSP, Consortium, and subcontractors under this Agreement shall be acquired in the name of the Purchaser and MSP shall have the non-exclusive, limited right to use such licenses till the Term on behalf of the Purchaser solely for the purpose of execution of any of its obligations under the terms of this Agreement. However, subsequent to the term of this Agreement, such approvals etc. shall endure to the exclusive benefit of the Purchaser.

2. **Bespoke Development:** Subject to provisions of Volume 3 Section 19 Clauses (1) and (4), the Purchaser shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have arisen out of or have been developed under the Scope of Work during execution of this Agreement, including but not limited to all processes, products, specifications, reports, drawings, applications, codes and other documents which have been newly created and developed by the MSP during the performance of the Services and for the purposes of, inter-alia, use or sub-license of such Services under this Agreement. The MSP shall provide source code, object code and all other relevant materials, artefacts etc. of all bespoke development to the Purchaser and the Purchaser shall own all IPRs in them. All material related to such bespoke development shall be treated as Confidential Information by the MSP. The MSP undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the Purchaser. The MSP shall execute all such agreements / documents and assist the Purchaser in filing all relevant applications, effect transfers and

obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the Purchaser at the cost of the Purchaser. Bespoke development shall include any customization or enhancement to COTS/third party products and, unless otherwise provided in the licensing terms of such COTS/third party products, the terms of this Volume 3 Section 19 Clause (2) shall apply to such customization or enhancement to COTS/third party products.

3. **License in Bespoke Development:** Upon receipt of written request from the MSP (or Consortium Partner), the Purchaser may grant license to MSP (or Consortium Partner) (hereinafter referred to as 'licensee' for purposes of this clause) to market, use, modify, enhance etc. the Bespoke Development. The terms of license agreement shall be mutually agreed between the licensee and the Purchaser. The license agreement shall, inter alia, define the royalty to be paid by the licensee to the Purchaser. Notwithstanding the foregoing, the royalty shall not be less than 10 (Ten) % of the payment to be received by the licensee in each project which involved any implementation etc. of the Bespoke Development. As a consideration for grant of license under this clause, the licensee shall also be obligated under the license agreement to replicate in the GeM Solution of the Purchaser, without any additional cost to the Purchaser, any enhancements, improvements etc. carried out by the licensee under any other project which involved any use implementation etc. of the Bespoke Development. The obligation to carry out such enhancements shall be limited to the term as agreed in the license agreement.

4. **Pre-existing work:** All intellectual property rights including the source code, tools, methodology, processes, ideas, know-how, technology existing prior to the Effective Date of this Agreement or developed independent of this Agreement, including any improvements, enhancements, modifications or customization made thereto or derivatives thereof developed independent of this Agreement (Pre- existing work), shall belong to the Party that owned such rights immediately prior to the Effective Date. Subject to the foregoing, the Purchaser will have a non- exclusive, transferable, perpetual, fully paid up, royalty-free, worldwide license to all pre-existing intellectual property rights of the MSP, Consortium Partner or subcontractors that are (i) provided or used by the MSP, Consortium, or subcontractors in providing services and goods under this Agreement; and/or (ii) incorporated in any deliverables, products, goods, or software provided by MSP, Consortium or subcontractors to the Purchaser under this Agreement.

5. **Ownership of documents:** The Purchaser shall own all Documents provided by or originating from the Purchaser and all Documents produced by or from or for the MSP in the course of performing the Services under this Agreement. Forthwith upon expiry or earlier termination of this Agreement and at any other time on demand by the Purchaser, the MSP shall deliver to the Purchaser all Documents provided by or originating from the Purchaser and all Documents produced by or from or for the MSP in the course of performing the Services, unless otherwise directed in writing by the Purchaser at no additional cost. The MSP shall not, store, copy, distribute or retain any such Documents in physical or electronic or in any other format without obtaining explicit written consent from the Purchaser. The MSP shall be wholly liable if any of its sub-contractors, agents, employees, consultants, etc. store/ retain/ copy/ distribute any of the documents which are directly or remotely pertaining to the services incorporated under this Agreement.

The MSP shall be permitted to retain information/documents as maybe required for legal or regulatory purposes, provided that the MSP shall strictly maintain confidentiality during such retention period and shall refrain from divulging such information/documents to any third party. The MSP shall not use the retained information/documents without express written consent from the Purchaser.

20. Warranty

1. The warranties and remedies provided in this Volume 3 Section 20 are in addition to, and not in derogation of, the warranties provided in Volume 1 of the RFP and the two are to be read harmoniously.

2. MSP shall provide ATS/AMC for the Software/solutions provided by the respective OEMs for the period specified in the RFP. The ATS should include upgrades, updates, and patches to the respective Software solution for the above stated period.

3. Warranty for Services – The MSP warrants that all services under this Agreement will be performed with promptness and diligence and will be executed in a workmanlike and professional manner, in accordance with the practices and high professional standards used in well-managed operations performing services similar to the services under this Agreement. The MSP represents that it shall use adequate numbers of qualified individuals with suitable training, education, experience, and skill to perform the services hereunder.

4. If the MSP, having been notified, fails to remedy the defect(s) within a reasonable period, the Purchaser may proceed, without prejudice to any other rights which the Purchaser may have against the MSP under the Agreement, to take such remedial action as may be necessary including invoking risk purchase as provided under Volume 3 Section 14.4 of this Agreement.

5. The representations, warranties and covenants provided by the MSP under this Agreement will not be affected by Purchaser's modification of any portion of the software so long as the MSP can discharge its obligations despite such modifications or following their removal by the Purchaser.

6. The MSP shall pass through all warranties and indemnities provided by the OEMs of COTS products / third party products and shall assist the Purchaser in claiming / effecting such warranties and indemnities. It is acknowledged by the Purchaser that the MSP will not provide any additional warranty with respect to such COTS products/third-party products.

21. Insurance Cover

21.1 Obligation to maintain Insurance

1. The MSP shall take out and maintain all insurances, against all the risks and in relation to this agreement and the scope of work and other obligations of this Agreement as mandated by the Applicable Law and / or by the Purchaser. The MSP, on demand made by the Purchaser, shall submit documentary evidence issued by the insurance company, indicating that such insurance has been taken by MSP/Consortium Partner/ sub-contractor(s).

22. Miscellaneous

22.1 MSP's Organization

1. The personnel assigned by the MSP to perform the Services shall under no circumstances be considered employees of the Purchaser or its nominated agencies. The MSP shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, provident fund, including salary, withholding of income taxes and social security taxes, worker's compensation, employee, and disability benefits and the like and shall be responsible for all obligations of an employer subject to the Applicable Law.

2. The MSP shall be fully responsible for the acts of its personnel/ representatives/ consultants/ team members/ consortium /sub-contractors/ employees and shall fully indemnify the Purchaser for any kind of losses or damages caused by its personnel/ representatives / consultants/ team members/ consortium/ sub-contractors/ employees. The Purchaser shall not be responsible for any claim from any personnel/ representatives / consultants/ team members/ consortium/ sub-contractors/ employee of the MSP. The MSP shall wholly and fully be responsible for any such claims.

3. The MSP shall ensure that the MSP's team is competent and professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Agreement in addition to the minimum qualification and experience as explained in Volume 1 Section 8.5.2 of this RFP.

4. The MSP shall appoint an employee as its authorized representative through a written notice to the Purchaser. The MSP's Representative shall have the authority to exercise all of the powers and functions of the MSP under this Agreement other than the power to amend this Agreement and ensure the proper administration and performance of the terms hereof and to bind the MSP in relation to any matter arising out of or in connection with this Agreement. The MSP, Consortium along with the Sub-Contractors/third parties shall be bound by all undertakings and representations made by the authorized representative of the MSP and any covenants stipulated hereunder, with respect to this Agreement, for and on their behalf. The MSP's representative shall have all the power requisite for the performance of the work under this Agreement. The MSP's Representative shall liaise with the Purchaser's Representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. The MSP's Representative will extend full co-operation to the Purchaser's representative for supervision/inspection/observation of the equipment/material procedures, performance, reports, and records pertaining to the works. The MSP shall comply with any instructions that are given by the Purchaser's representative during the course of this Agreement in relation to the performance of its obligations under the terms of this Agreement and the RFP. MSP's Representative shall also have complete charge of the MSP's personnel engaged in the performance of the works and to ensure compliance of rules, regulations, and safety practice. MSP's Representative shall also cooperate with the other service providers/contractors of the Purchaser. Such MSP's representative shall be available to the Purchaser's Representative during the execution of Services.

5. The MSP shall, to the best of its efforts, avoid any change in the organizational structure proposed for execution of this Agreement or replacement of any manpower resource appointed. If the same is however unavoidable, for reasons and circumstances such as death, medical incapacity, resource leaving MSP's organization, the same shall be notified to the Purchaser immediately or at least 30 (Thirty) days prior to resource leaving the Project. Any resource absent for a period greater than or equal to 30 (Thirty) days shall be considered for replacement by the MSP, unless otherwise approved by the Purchaser. The MSP shall promptly inform the Purchaser in writing if any such revision or change is necessary. In case of replacement of any manpower resources, the MSP shall replace the resource with a better or equally competent resource within 30 (Thirty) days (extendable up to a total of 60 (Sixty) days with the consent of the Purchaser) of the resource's resignation/ absence/ termination. The MSP shall ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand holding period and training for the incoming resource. The change or revision of resources, and delay in replacing the resources from agreed upon timelines, shall be subject to levy of Liquidated damages as provided in the Volume 1 Section 3.3.3 of this RFP. Liquidated damages as provided in the Volume 1 Section 3.3.3 of this RFP shall not be applicable in case of replacement of resource is due to approved leaves by the MSP and Purchaser on account of maternity leave, paternity leave, serious medical conditions certified by a reputed medical practitioner and approved by the Purchaser, and demise of the resource.

6. The Purchaser's Representative may at any time request the MSP to remove from the Services any employee of the MSP or its sub-contractor or any person(s) deployed by the MSP or its sub-contractor or consortium partner for professional incompetence or negligence or for being deployed for work for which he/she is not suited or for unethical, corrupt, fraudulent behaviour. The MSP shall consider the Purchaser's Representative request and may accede to or disregard it except that in case of unethical, corrupt, fraudulent behaviour, the MSP shall remove the person immediately. The Purchaser's Representative, having made a request, as aforesaid in the case of any person, which the MSP has disregarded earlier, may in the case of the same person at any time but on a different occasion, and for a different instance of one of the reasons referred to above in this Clause object to and require the MSP to remove that person from deployment on the work, which the MSP shall then forthwith do and shall not again deploy any person so objected to, for any work which is directly or remotely related to Scope of Work as stipulated in Volume 1 of this RFP without the explicit written consent of the Purchaser's Representative. The Purchaser's Representative shall state to the MSP in writing his reasons for any request or requirement pursuant to this clause. The MSP shall replace every person removed, pursuant to this section, with a competent substitute within 30 (Thirty) days of removal (extendable up to a total of 60 (Sixty) days with the consent of the Purchaser), and at no extra cost to the purchaser. Any delay from agreed upon timelines in replacing the resources removed shall be subject to levy of Liquidated damages as provided in Volume 1 Section 3.3.3 of this RFP.

7. The MSP's obligation to render its services onsite (from the Purchaser's Premises) or offsite (from MSP manages facilities) shall be subject to any applicable government restrictions that may be imposed by any government authorities by way of any government orders/notifications/circulars or any other mode for reasons such as prevention of outbreak of pandemic etc. On occasion of any such government restrictions which may directly or indirectly hinder in rendering of services at the physical location of the Purchaser, the

Purchaser shall allow the MSP to render its services from remote location for such period till the government restrictions are waived off by any further government orders/notifications/circulars.

22.2   Independent Contractor

Nothing in this Agreement or the SLA shall be construed as establishing or implying any partnership or joint venture between the Parties to this Agreement and, except as otherwise provided in this Agreement or any Power of Attorney given by Consortium Partner to the Lead Bidder, nothing in this Agreement shall be deemed to constitute any Parties as the agent of any other Party or authorizes either Party to:

1. Incur any expenses on behalf of the other Party;

2. Enter into any engagement or make any representation or warranty on behalf of the other Party;

3. Pledge the credit of or otherwise bind or oblige the other Party; or

4. Commit the other Party in any way whatsoever without in each case obtaining the other Party's prior written consent.

22.3   Sub-contractors

1. Except for subcontracting allowed in Volume 2 Section 1.1 of the RFP, the MSP shall not subcontract any part of the scope of work under this Agreement to any third party without the prior written consent of the Purchaser, which consent shall not be unreasonably delayed or withheld. MSP shall assist the Purchaser with all documents etc. required by the Purchaser to decide whether to give its consent or not. While giving its consent for appointment of any subcontractor, the Purchaser may impose such conditions on subcontracting as mutually agreed between the MSP and the Purchaser for successful accomplishment of the obligations of the MSP under this Agreement and such conditions shall be applicable on the MSP and the subcontractor (as applicable).

2. Prior to executing any contract or entering into any contract or understanding with a sub-contractor, the MSP shall ensure that, where requested by the Purchaser, the sub-contractor appointed by the MSP executes a non-disclosure agreement and a deed of adherence in the manner and form prescribed by the Purchaser. The deed of adherence will be a unilateral undertaking from the subcontractor to the Purchaser. The terms of deed of adherence shall be discussed by the Purchaser with the MSP. Execution of deed of adherence by the subcontractor shall not in any way relieve the MSP from any of its obligations and liability under this Agreement.

3. The MSP shall ensure that the subcontractor proposed by MSP is competent and professional and possess the requisite qualifications and experience appropriate to the tasks they will perform under this Agreement.

4. Any change of the sub-contractor(s), after the arrangement is firmed up, will be made by the MSP only with the prior written approval of the Purchaser which approval shall not be unreasonably withheld or delayed.

5. The MSP shall be responsible and shall ensure the proper execution and performance of the services or tasks so sub-contracted and shall be liable for any non-performance or breach by such sub-contractor. The MSP indemnifies, defends, and hold harmless and shall keep indemnified the Purchaser against any losses, damages, claims or such other implications arising from or out of the acts and omissions of such sub- contractor. It is clarified that this indemnity refers to (a) the same extent and nature the MSP is liable to indemnify for MSP's own acts and omissions under this Agreement; and (b) any claims made by the subcontractor against the Purchaser due to breach by the MSP of the agreement entered into between subcontractor and the MSP. The MSP shall be responsible for making all payments to the sub- contractor as may be necessary, in respect of any work performed or task executed, and the Purchaser shall not be responsible for any part or full payment, which is due to such sub-contractor.

6. The clauses related to intellectual property rights applicable on the MSP under this Agreement shall be mutatis mutandis applicable to the deliverables/services etc. provided by the sub-contractors. The MSP should provide the undertakings given by the subcontractor within 30 (Thirty) days from the date of appointment of subcontractor to disclose all such Intellectual Property Rights arising in performance of the Services to the Purchaser and execute all such agreements/documents and file all relevant applications, effect transfers, and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the Purchaser.

7. Nothing in this Agreement or any subcontract agreement hereunder shall relieve the MSP from its liabilities or obligations under this Agreement to provide the Goods and Services in accordance with this Agreement.

8. Where the Purchaser deems necessary, it shall have the right to require replacement of any sub-contractor with another sub-contractor and the MSP shall in such case find of the suitable replacement for such sub-contractor to the satisfaction of the Purchaser at no additional charge. Failure on the part of the MSP to find a suitable replacement shall amount to a breach of the terms hereof and the Purchaser in addition to all other rights, have the right to claim damages and recover from the MSP all losses/or other damages that may have resulted from such failure. In case the MSP terminates any contract / arrangement or agreement with a sub-contractor for any reason whatsoever, the MSP shall ensure the smooth continuation of Services by providing forthwith, a suitable replacement which is acceptable to the Purchaser at no additional charge. In case of a replacement of the sub-contractor, the new sub-contractor shall have the qualification at least as good as the replaced subcontractor.

22.4   MSP's Obligations

The obligations of the MSP described in this clause are in addition to, and not in derogation of, the obligations mentioned in Volume 1 of this RFP and the two are to be read harmoniously:

1. The MSP shall be the sole point of contact for all matters relating to this RFP and Agreement thereof.

2. The MSP shall ensure that the MSP's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Agreement. The MSP shall ensure that the Services are performed through the efforts of the MSP's Team, in accordance with the terms hereof and to the satisfaction of the Purchaser. Nothing in this Agreement relives the MSP from its liabilities or obligations under this Agreement to provide the Services in accordance with the Purchaser's direction and requirements and as stated in this Contract and the performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of MSP's Team.

3. The MSP's Representative(s) shall have all the power requisite for execution of Scope of Work and performance of services under this Agreement. The MSP's Representative(s) shall liaise with the Purchaser's Representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. MSP's Representative(s) should extend full co-operation to the Purchaser's Representative for the proper coordination and timely completion of the works and on any other matter pertaining to the works. MSP's Representative(s) should extend full co-operation to Purchaser's Representative in the manner required by them for supervision/inspection/observation of the equipment/goods/material, procedures, performance, progress, reports ad records pertaining to the works. MSP's Representative(s) shall also have complete charge of the MSP's personnel engaged in the performance of the works and to ensure compliance of rules, regulations, and safety practice. MSP's Representative(s) shall also cooperate with other Service Providers/Vendors of the Purchaser.

4. The MSP shall at all times ensure that the services being provided under this Agreement are performed strictly in accordance with all applicable laws, notifications, guidelines, orders, byelaws, regulations, rules, standards, recommended practices etc., and no liability in this regard will be attached to the Purchaser.

5. MSP shall provide the Purchaser or its nominated agency access to or a copy of any information, document, data, etc. for any legal, compliance, audit, or regulatory matter promptly on a request made by the Purchaser or its nominated agency.

6. MSP shall ensure that all information, data, documentation, etc. provided by the MSP or its consortium partners or sub-contractors or any of its representative, to the Purchaser is true and accurate. In case the information, data, documentation etc. shared is found to be incorrect or inaccurate, it shall be treated as an event of default and shall be governed by Volume 3 Section 13 of this RFP. In case this incorrect or inaccurate information/ data/ documentation shared was used to calculate the fee amount payable to the MSP, then Purchaser reserves the right to re-calculate the fee amount payable to the MSP and recover any amount paid over and above the re-calculated fees previously.

22.5 Assignment

1. All terms and provisions of this Agreement shall be binding on and shall inure to the benefit of the Purchaser, the MSP, the Consortium Partner, and their respective permitted successors and permitted assigns.

2. The MSP and Consortium Partner shall not be permitted to assign or transfer any or all of its rights and obligations under this Agreement to any third party without the prior written permission of the Purchaser.

3. Subject to the foregoing, the MSP and Consortium Partners shall have the right to undergo corporate change of ownership through mergers, demergers, slump sale etc., as allowed under Applicable Laws, after seeking prior written consent from the Purchaser. The Purchaser shall convey its consent or dissent within 30 (Thirty) days from date of receipt of request from the MSP/Consortium Partner. If the Purchaser fails to convey its consent or dissent within such 30 (Thirty) days period, it shall be deemed that the Purchaser has given its consent. The MSP or Consortium Partner shall execute/furnish such documents, agreements, undertakings (including, without limitation, enhanced performance security from new entity, novation agreements etc.) as may be deemed necessary by the Purchaser, at no additional cost to the Purchaser.

4. Parties acknowledge that the Purchaser may set up an entity such as an autonomous body etc. to, inter alia, take over and manage the Project. Parties agree that the Purchaser shall have the right to assign and novate all or any part of this Agreement and Schedules/Annexures etc. to such separate entity autonomous body after giving 15 (Fifteen) days written notice to the MSP. The MSP and Consortium Partners agree that they shall forthwith execute, without demur, all such agreements and documents as may be requested by the Purchaser to give effect to such assignment novation.

22.6 Trademarks, Publicity

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that the MSP may include the Purchaser or its client lists for reference to third parties subject to the prior written consent of the Purchaser not to be unreasonably withheld or delayed. Such approval shall apply to each specific case and relate only to that case.

22.7   Notices

Any notice requests, demands or communications to be made under this Agreement shall be in writing and shall either be delivered personally, or sent by registered post / recognized courier service or via email.

1. In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

   Purchaser:

   Addressee:

   Address:

   Tel:

   Email:

   MSP

   Addressee:

   Address:

   Tel:

   Email:

2. In relation to a notice given under this Agreement, a Party shall specify the Party's address for service of notices, any such notice to be copied to the Parties at the addresses set out in this Clause.

3. Any such notice or other document shall be deemed to have been given to the other Party (or, if relevant, its relevant associated company) when delivered (if delivered in person) or sent by email, if delivered between the hours of 9.00 am and 5.00 pm at the address of the other Party set forth above or, or on the next working day thereafter if delivered outside such hours, and 7 (Seven) days from the date of posting (if by letter).

4. Either Party to this Agreement may change its address, telephone number, facsimile number and nominated contact for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

22.8   No Claim Certificate

1. The MSP shall not be entitled to make any claim, whatsoever against the Purchaser under or by virtue of or arising out of, this contract/ agreement, nor shall the Purchaser entertain or

consider any such claim, if made by the MSP after he/she shall have signed a 'No claim' certificate in favour of the Purchaser in such forms as shall be required by the Purchaser after the works are finally accepted.

22.9   Severability and Waiver

1. If any provision of this Agreement, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid, or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid, or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal, and commercial objectives of the illegal, invalid, or unenforceable provision or part provision.

2. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement of any right, remedy or provision of this Agreement shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

3. Any waiver of rights, powers, or remedies under this Agreement must be in writing, dated, and signed by an authorized representative of the Party granting such waiver and must specify the terms under which the waiver is being granted

22.10   Compliance with Applicable Law

1. The MSP shall comply with the provision of all laws including labour laws, rules, regulations, and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the Purchaser shall be applicable in the performance of this Agreement and the MSP shall abide by these laws. The MSP shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. The MSP shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations. The MSP shall also adhere to all security requirement/regulations of the Purchaser during the execution of the work.

2. Each Party to this Agreement accepts that its individual conduct shall (to the extent applicable to its business - like if the MSP is an Information Technology service provider, then MSP has to follow laws applicable to it as an Information Technology service provider and if the Consortium Partner is an e-commerce services provider, then the Consortium Partner has to follow laws applicable to it as an e-commerce services provider) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be dealt with

in accordance with the Change Control Procedure set out in Volume 1 Section 8.7 of this RFP.

3. During the tenure of this Agreement, the MSP shall comply with all Applicable Laws and shall obtain and maintain all statutory and other approvals required for the performance of the Services under this Agreement and nothing shall be done by the MSP or any of the Consortium Partner in contravention of any Applicable Law or any amendment thereof.

22.11   Professional Fees

1. All expenses incurred by or on behalf of each Party to this Agreement, including all fees of agents, legal advisors, accountants, and actuaries employed by either of the Parties in connection with the negotiation, preparation and execution of this Agreement shall be borne solely by the Party which incurred them.

22.12   Ethics

1. The MSP and Consortium Partner, for itself and on behalf of its subcontractors, agents, representatives, employees etc., represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee or agent of the Purchaser or its nominated agencies in connection with this Agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of the Purchaser's standard policies and may result in cancellation of this Agreement.

22.13   Amendment

Any amendment to this Agreement shall be made in writing by mutual consent of the Parties.

22.14   Conflict of Interest

1. The MSP shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise, or may arise (either for the MSP, Consortium Partner or the MSP's or Consortium Partner's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

    a. The MSP shall be able to offer goods and services of the MSP on GeM portal provided the following are met:

    b. MSP shall provide complete and full disclosure of its (or any of its parent of subsidiary or affiliate company) interest in any goods and services MSP proposes to offer on the GeM Portal to the Board of Directors (BoD) of the GeM (or any committee constituted by the BoD in this regard) as applicable;

2. MSP shall follow the process agreed between GeM and MSP as per Volume 3 Section 24.14

to ensure fairness, competition, and transparency in relation to goods and services being proposed to be offered by the MSP;

(The interest mentioned above includes, without limitation, any interest by way of an agreement the nature of which is to promote goods and services of any particular seller(s).)

3. It is the intention of the parties that the Purchaser and the MSP shall, within 120 (One Hundred and Twenty) days of signing of the Agreement, mutually agree on a standard process and measures, that the MSP will need to follow before offering its or any consortium partners or subcontractors (or any of their parent or subsidiary or affiliate company) goods and services on the GeM portal to ensure that such goods/services would not get any special preferential treatment on the portal and would be treated at par with goods and services offered by other sellers.

22.15   Survival

Any provision of this Agreement which imposes or intends to impose an obligation on any of the Parties after termination or expiration of this Agreement shall survive the termination or expiration of this Agreement. Such provisions include, without limitation, obligations related to confidentiality, indemnity, licenses, risk purchase and AMC/ATS, if any, to be provided by the OEMs or the MSP.

23. Bank Guarantees

1. Performance bank guarantee

    a. The MSP shall furnish, within 15 (Fifteen) days from the date of the receipt of the notification of award, an unconditional, irrevocable, and continuing Bank Guarantee, in the format as per Volume 2 Section 4.6 of this RFP, from a scheduled bank in India, equivalent to 3% of the total estimated contract value as mentioned in this RFP, which should remain valid till 6 (Six) months beyond expiry of the Term of the Agreement (Performance Guarantee).

    b. In the event of the MSP being unable to service the Agreement for reasons attributable to the MSP, its consortium partners or any subcontractors, or any team members, the Purchaser shall have the right to invoke the Performance Guarantee. Notwithstanding and without prejudice to any rights whatsoever of the Purchaser under the Agreement in the matter, the proceeds of the guarantees shall be payable to the Purchaser as compensation for any loss resulting from the failure of MSP, its consortium partners or any subcontractors, or any team members to perform/comply its obligations under the contract. The Purchaser shall notify the MSP in writing of the exercise of its right to receive such compensation within 30 (Thirty) days, indicating the contractual obligation(s) for which the MSP is in default.

    c. The Purchaser shall also be entitled to make recoveries from the MSP's bills, guarantees, or from any other amount due to him, an equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction, or misstatement.

    d. In case the Project is delayed beyond the Timelines as mentioned in this RFP due to reasons attributable to MSP, its consortium partners or any subcontractors, or any team members, the Performance Guarantee shall be accordingly extended by the MSP till completion of scope of work as mentioned in this RFP.

    e. If the MSP fails to provide the Purchaser an extended/ replacement Performance Bank Guarantee in accordance with this clause at least thirty (30) days prior to the date of expiry of the then existing Performance Bank Guarantee, the Purchaser shall be entitled to draw the full amount of the Performance Bank Guarantee then available for drawing and retain the same until such time as the Purchaser shall receive such an extended/ replacement Performance Bank Guarantee, whereupon, subject to this Agreement, the Purchaser shall refund to the MSP the full amount of Performance Bank Guarantee, unless the Purchaser has drawn upon the Performance Bank Guarantee in accordance with the provisions of this Agreement, in which case only the balance amount remaining will be refunded to the MSP; provided that the Purchaser shall not be liable to pay any interest on such balance. The Purchaser shall return the Performance Bank Guarantee to the issuer for cancellation promptly upon receipt of any extension/ replacement thereof.

24. Constitution of consortium

1. For the purposes of fulfilment of its obligations as laid down under the Agreement, unless the context requires otherwise, MSP shall be the sole point of interface between the Purchaser and the MSP and the MSP would be absolutely accountable for the performance of its own, the other members of Consortium and or its Team's functions and obligations.

2. The Consortium Partners agree that the MSP shall be the prime point of contact between the Consortium Partners and the Purchaser and shall be primarily responsible for the discharge and administration of all the obligations contained herein and, the Purchaser, unless it deems necessary shall deal only with the MSP.

3. MSP shall not, except with the prior approval of the Purchaser, have any provision in the consortium agreement or make any amendments to the said consortium agreement which adversely affects the rights and/or obligations of MSP and Consortium Partners under this Agreement or any amendment which is contrary to the provisions of this Agreement.

4. The MSP and Consortium Partners shall be jointly and severally liable for all obligations under this Agreement. Notwithstanding the foregoing, in case of a breach of any of the terms hereof, the Consortium Partner shall be responsible and liable only for obligations related to goods and services to be supplied by the Consortium Partner and the MSP shall be, in addition to its own obligation, responsible and liable for the obligations of the Consortium Partners. Notwithstanding the foregoing and subject to clause 14.6 of the Agreement, the liability for direct damages of each Consortium Partner under this Agreement shall be limited to the total amount corresponding to and commensurate with the scope of work related to the Consortium Partner and the liability for direct damaged of the Lead Bidder shall be limited to as per the limitation of liability clause 14.3. The Lead Bidder shall ensure that at all times during the Term of this Agreement, each member of the Consortium and the Implementation Partner's Team complies with all the terms and conditions of this Agreement. Provided that MSP may, if it deems necessary, deal with only the Lead Bidder or any member of the Consortium, individually or as a group.

5. The Lead Bidder shall ensure that at all times during the Term of this Agreement, Consortium Partner and the Consortium Partner's Team complies with all the terms and conditions of this Agreement. A Power of Attorney in favor of the authorized signatory shall be signed and submitted with bid proposal (as per attached format in Volume 2 Section 4.3.9 and 4.3.10 in this RFP).

6. The MSP and the Consortium Partner shall be bound by all undertakings and representations made by their authorized representative and any covenants stipulated hereunder with respect to this Agreement, for and their behalf. The terms and conditions of this Agreement shall mutatis mutandis apply to all Consortium Partners.

7. The MSP shall not change any Consortium Partner without the prior written approval of the Purchaser. The approval of the Purchaser may be subject to certain conditions in terms of credentials and qualifications of the new Consortium Partner which the MSP shall be liable to meet. The MSP shall give a notice of at least 3 (Three) months in advance to the Purchaser if during the term of this Agreement the MSP desires to terminate any contract/arrangement

relating to the performance of Services hereunder with the Consortium Partner. Where, during the term of this Agreement, the MSP terminates any contract/arrangement or agreement relating to the performance of the Services hereunder with any Consortium Partner (subject to approval by the Purchaser), the MSP shall be liable for any consequences resulting from such termination. The MSP shall in such case ensure the smooth continuation of Services by providing a suitable replacement subject to approval and to the satisfaction of the Purchaser at no additional charge and at the earliest opportunity.

25. Governing Law and Dispute Resolution

A.   AMICABLE SETTLEMENT:

In the event of any conflict or dispute arising out of or in connection with the Agreement, the Parties (i.e., the MSP and the Purchaser) shall endeavor to settle such disputes amicably. If a dispute is not resolved within 30 (thirty) days after a written notice of any dispute by one Party to the other, the dispute shall then be referred to Arbitration.

B.   ARBITRATION:

In the event of any conflict / dispute arising out of or in connection with the Agreement, which has not been amicably resolved, the aggrieved Party may invoke Arbitration by sending a written notice to the other Party. The procedure for appointment of the Arbitral Tribunal shall be as follows.

1. The arbitration shall be conducted by a quorum of three arbitrators. Each party shall be entitled to appoint an arbitrator and the two party-appointed arbitrators shall within 30 (Thirty) days from their nomination, appoint a third arbitrator i.e., the Presiding Arbitrator.

2. The arbitration shall be conducted in the English language. Arbitration proceedings can also be conducted online, as per the discretion of the Arbitral Tribunal.

3. The cost of the Arbitration shall be equally borne by both the Parties.

4. The award of the Arbitral Tribunal shall be final and binding on the Parties to the Agreement. The arbitration shall be governed by the provisions of the Arbitration and Conciliation Act, 1996, as amended up to date. The seat of arbitration shall be at New Delhi, India.

5. Where the arbitral award is for the payment of money, no interest shall be payable on whole or any part of the money for any period till the date on which the award is made.

6. The Agreement shall be interpreted and governed in all respects in accordance with the laws of India. All disputes in connection with or arising out of the Agreement, shall be subject to the exclusive jurisdiction of the Courts at New Delhi.

7. The MSP shall not be entitled to suspend the Service/s or the completion of the work, pending resolution of any dispute between the Parties and shall continue to render the Service/s in accordance with the provisions of the Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration, court, or other proceedings.

IN WITNESS WHEREOF the Parties have by duly authorized Representatives set their respective hands and seal on the date first above Written in the presence of:

For and on behalf of Government e-Marketplace (FIRST PARTY)

[Name and Designation]

For MSP (SECOND PARTY)

[Name and Designation]

WITNESSES:

1.   [Signature, Name and Address]
2.   [Signature, Name and Address]

26. Schedule I - Definitions

1. 'Acceptance' - a hardware, software, solution (including GeM Solution), or any other deliverable shall be considered to have been accepted by the Purchaser, subsequent to its Commissioning and Testing, when all the activities as defined in Volume 1 Section 3.1.2.8 & 3.1.2.9 and Volume 3 Section 8 of this RFP have been successfully executed and completed by the MSP and the Purchaser has indicated his acceptance by signing the Acceptance Certificate.

2. 'Acceptance Certificate' - means that document issued by the Purchaser signifying Acceptance of a hardware, software, solution (including GeM solution), or any other deliverable pursuant to the successful completion of the Acceptance Test of the System.

3. 'Acceptance Test Plan' shall have the meaning given in Volume 1 Section 3.1.2.8 & 3.1.2.9 of this RFP.

4. 'Applicable Law(s)' means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, byelaw, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;

5. 'Assets' shall have the same meaning ascribed to it in Volume 3 Section 9.1 (1);

6. 'MSP' or 'Lead Bidder' shall have the meaning ascribed to such term in Parties clause of this Agreement and shall be deemed to include the MSP's successors, representatives (approved by the Purchaser), heirs, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the contract/ agreement. The word MSP when used in the pre-award period shall be synonymous with parties bidding against this RFP

7. 'MSP's Team' means the MSP along with all of its Consortium Partners, who have to provide Goods and Services to the Purchaser under the scope of this Agreement. This definition shall also include any and/or all of the employees of the MSP, Consortium Partners, authorized partners/agents and representatives or other personnel employed or engaged either directly or indirectly by the MSP for the purposes of this Contract/ agreement.

8. 'Change Request' or 'Change Order' or 'Alteration' or 'Variation' shall have the meaning given in Volume 1 Section 8.7 of this RFP hereof.

9. Confidential Information' means any and all data and information whether contained in any tangible medium of expression or in visual form, disclosed to or by any Party pursuant to this Agreement and includes without limitation information which:

   a. is by its nature confidential or by the circumstances in which it is disclosed confidential; or

    b. is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is available lawfully in the public domain.

10. 'Document' means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes or any databases or microfilm or computer-generated micro fiche.

11. 'Effective Date' shall have the same meaning ascribed to it in Volume 3 Section 3;

12. 'Fees' means the amount payable to MSP in Indian Rupees.

13. 'Force Majeure' shall have the same meaning ascribed to it in Volume 3 Section 15.1;

14. 'Go Live' means completion of Go Live activities as mentioned in Volume 1 Section 5 of this RFP and acceptance of the same by the Purchaser.

15. 'Intellectual Property Rights IPR' means any patent, copyright, trademark, trade name, design, trade secret, permit, service marks, brands, proprietary information, knowledge, technology, licenses, databases, computer programs, software, know-how or other form of intellectual property right, title, benefits or interest whether arising before or after the execution of this Agreement and the right to ownership and registration of these rights.

16. ''Notice' means:

    a. a notice; or

    b. a consent approval or other communication required to be in writing under this Agreement, to be served at the addresses as given under clause hereunder.

17. 'A' mean the bidding parameter value quoted by the MSP in the commercial bid format.

18. 'Performance Guarantee' means the guarantee to be provided by the MSP as per Volume 3 Section 4.2 of the Agreement.

19. 'Purchaser's Material' shall have the meaning ascribed to such term in Volume 3 Section 5.2 (5) of the Agreement

20. Purchaser's Representative Project Coordinator' means the person, or the persons appointed by the Purchaser from time to time to act on its behalf for overall coordination, supervision, and project management.

21. 'RFP' shall have the meaning ascribed to such term in the WHEREAS clause of this Agreement.

22. "Scope of Work" means all Services, and any other deliverables as required to be provided by the MSP as specified in Volume I of this RFP.

23. 'Services' means the services to be provided as per the requirements conditions specified in

the Scope of Work and the Agreement. In addition to this, the definition would also include other related ancillary services that may be required to execute the Scope of Work under this Agreement.

24. 'Service Level(s)' means the service level parameters and targets and other performance criteria which will apply to the Services and Deliverables as described in Volume 1 of this RFP; 'SLA' or 'Service Level Agreement' means the service level agreement specified in Volume 1 of this RFP;

25. 'Service Specifications' means and includes detailed description, statements to technical data, performance characteristics, and standards (Indian as well as International) as applicable and as specified in the Agreement, as well as those specifications relating to industry standards and codes applicable to the performance of work, work performance quality and specifications affecting the work, or any additional specifications required to be produced by the MSP to meet the design criteria.

26. 'System' means integrated system/solution emerging out of the Scope of Work and covered under the scope of each Purchase Order issued by the Purchaser.

27. 'Term' shall have the same meaning ascribed to it in Volume 3 Section 3;

28. 'Timelines' means the project milestones for performance of the Scope of Work and delivery of the Services as described in Volume 1 of this RFP;

29. CSP shall abide by all laws,/ rules / regulations/ notifications/ guidelines/ orders issued by any department/ ministry / office of the Government of India

27. Schedule II – Audit, Access, and Reporting

1. **PURPOSE**

   This Schedule details the audit, access and reporting rights and obligations of the Purchaser or its nominated agency and the MSP. This Schedule is in addition to, and in derogation of, the audit rights and process provided in the RFP.

2. **AUDIT NOTICE AND TIMING**

   a. As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavours to agree to a timetable for routine audits (Other than those mentioned as part of the mandatory requirements for successful execution of the Engagement) during the entire duration of the Engagement.

   b. The Purchaser may conduct non-timetabled audits at his/her own discretion, if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the MSP, a security violation, or breach of confidentiality obligations by the MSP, provided that the requirement for such an audit is notified in writing to the MSP a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based. If the MSP considers that the non-timetabled audit was not appropriate, the matter shall be referred to the escalation procedure as set out in the Project Governance and Management section of RFP.

   c. Except as provided in Volume 3 Section 27 Clause (2b) above, audits shall be conducted by with adequate notice of 2 (Two) weeks to the MSP.

3. **ACCESS**

   The MSP shall provide to the Purchaser or its nominated agency reasonable access to employees, subcontractors, suppliers, agents, and third-party facilities (excluding CSP) as detailed in the RFP, documents, records, and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The Purchaser or its nominated agency shall have the right to copy and retain copies of any relevant records. The MSP shall make every reasonable effort to co-operate with them.

4. **AUDIT RIGHTS**

   The Purchaser or its nominated agency shall have the right to audit and inspect suppliers, agents, and third-party facilities (excluding CSP facilities) (as detailed in the RFP), documents, records, procedures, and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

a. The security, integrity and availability of all data processed, held, or conveyed by the Partner on behalf of the Purchaser and documentation related there to;

b. That the actual level of performance of the services is the same as specified in the SLA;

    i. That the MSP has complied with the relevant technical standards, and has adequate internal controls in place;

    ii. MSPs deployment of resources and their attendance records;

    iii. MSP's internal testing results; and

    iv. The compliance of the MSP with any other obligation under the Agreement;

For the avoidance of doubt the audit rights under this Schedule shall not include access to the MSP's profit margins or overheads, any confidential information relating to the MSP' employees, or (iii) minutes of its internal Board or Board committee meetings including internal audit, or (iv) such other information of commercially confidence in nature which are not relevant to the Services associated with any obligation under the Agreement.

5. **AUDIT RIGHTS OF SUPPLIERS AND AGENTS**

a. The MSP shall use reasonable endeavours to achieve the same audit and access provisions as defined in this Schedule with suppliers and agents who supply labour, services, equipment, or materials in respect of the services. The MSP shall inform the Purchaser or its nominated agency prior to concluding supply agreement of any failure to achieve the same rights of audit or access.

b. The MSP shall ensure that the Purchaser or its nominated agency shall, at any point of time, have remote access (including provision through a console) to its facilities to conduct the audit of the provisioned cloud services, including underlying infrastructure. The Purchaser or its nominated agency shall have the right under Clause 3 and 4 of this Schedule if such access and audit is required under any applicable law.

c. **REPORTING:** The MSP will provide quarterly reports to the Purchaser or its nominated agency regarding any specific aspects of the Project and in context of the audit and access information as required by the Purchaser or its nominated agency.

6. **ACTION AND REVIEW**

a. Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to the Purchaser or its nominated agency and the MSP's representative shall inform the Purchaser about the actions that would be taken by the MSP in respect of such discrepancies within a period of thirty (30) calendar

days from the submission of the said audit assessment report or such earlier time period as notified by the Purchaser.

b. Any change or amendment to the systems and procedures of the MSP, where applicable, arising from the audit assessment report shall be agreed within thirty (30) calendar days from the submission of the said audit assessment report or such earlier time period as notified by the Purchaser. The changes agreed by the Purchaser, or any changes suggested by the Purchaser, shall be implemented by the MSP within a period of not more than 30 (Thirty) days or such other period as may be requested by the MSP and agreed to by the Purchaser.

7. **TERMS OF PAYMENT**

Except for the audits that are required to be conducted by the MSP as provided in Volume 1 of this RFP for which the costs will be borne by the MSP, the Purchaser shall bear the cost of other audits and inspections. The MSP shall bear all costs for all reasonable assistance and information provided under the Agreement, Project Implementation, Operation and Maintenance SLA by the MSP pursuant to this Schedule.

8. **RECORDS AND INFORMATION**

For the purposes of audit in accordance with this Schedule, the MSP shall maintain true and accurate records in connection with the provision of the services and the MSP shall handover all the relevant records and documents upon the termination or expiry of the Agreement.

The MSP at all times make and keep sufficient copies of the Agreement documents, manuals, reference material, drawings, specifications, and any other document required by him to fulfil his duties under this Agreement.

28.   Schedule III – Project Deliverables and Timelines

As per Volume 1 Section 5 of this RFP

29. Schedule IV – Exit Management Schedule

'Exit Management and Transition' would include any event/series of activities with prior written approval from the Purchaser which results in transfer of any/all data/ knowledge/ operations/ processes/ documentation/ assets/ personnel, etc from the outgoing MSP to the Purchaser/ incoming MSP/ any agency appointed by the Purchaser at the time of termination or expiry of the MSP's contract/ agreement.

MSP shall be responsible for exit management and transition to any agency appointed by the Purchaser. The scope of activities for exit management and transition, at a minimum, shall be as outlined in Volume 1 Section 3.5 of this RFP.

Annexure A – Non-Disclosure Agreement

<u>CORPORATE NON-DISCLOSURE AGREEMENT</u>

This Non-Disclosure Agreement ("Agreement") is entered on this <*** >day of <***>, 2022

By and between

Government e Marketplace (GeM), Ministry of Commerce and Industry, Government of India, having its office located at 3ʳᵈ Floor, Tower II, Jeevan Bharti Building, Connaught Place, New Delhi (herein after referred to as *"Purchaser"*, which expression shall unless excluded by or repugnant to the context deemed to include its successor/s in office or assign);

And

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter called the *"Receiving Party" / "Managed Service Provider"/ "MSP" / "Lead Bidder")*, which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its successors and permitted assigns).
And

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter called the "Receiving Party" / "*Consortium Partner*", which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its successors and permitted assigns).

And (if applicable)

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter called the "Receiving Party" / "*Consortium Partner*", which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its successors and permitted assigns).

(GeM, MSP, and Consortium Partner(s) shall be individually referred hereinafter as *"Party"* and collectively as *"Parties"*).
/

Background

1. The Parties have entered into an Agreement dated <***>, 2022 (here in after referred as "Master Service Agreement" or "MSA"), wherein <***> has been engaged for providing _____(the "Purpose").

NOW THEREFORE, in consideration of the mutual agreements and covenants hereinafter set forth, GeM and MSP and Consortium Partner(s), hereby agree as follows:

1. In course of MSP and Consortium Partner(s)'s engagement with GeM, MSP and Consortium Partner(s) shall be exposed to Confidential, proprietary, and highly sensitive information relating to GeM. "Confidential Information" shall mean all information and data disclosed by GeM ("***Disclosing Party/ Discloser***") to MSP and Consortium Partner(s) ("***Receiving Party/ Recipient***"), or any information Receiving Party becomes aware of / obtains /possess during his/her engagement with GeM, whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including but not limited to;

   a. Intellectual property

   b. Trade secrets;

   c. Proprietary information related to the current, future, and proposed products and services of the Disclosing Party including, without limitation, technical data, research, mask works, ideas, samples, media, techniques, sketches, drawings, works of authorship, models, inventions, know-how, processes, apparatuses, equipment, algorithms, software codes and designs, software programs, software source documents, and formulae, its information concerning research, experimental work, development, design details and specifications, engineering, financial information, procurement requirements, purchasing, manufacturing, customer lists/information, investors, employees, business and contractual relationships, business forecasts, sales and merchandising, marketing plans, price lists, pricing methodologies, cost data, market share data, licenses, contract information, business plans, financial forecasts, historical financial data, budgets, GeM transactions data, demographic details, information regarding third parties or other business information disclosed by GeM either directly or indirectly, whether in writing, electronically, orally, or by observation.

   d. Information and physical material not generally known or available outside GeM and information and physical material entrusted to GeM in confidence by third parties.

   e. Inventions such as discoveries, developments, concepts, designs, ideas, know how, improvements, inventions, trade secrets and/or original works of authorship, whether or not patentable, copyrightable, or otherwise legally protectable. This includes, but is not limited to, any new product, machine, article of manufacture, biological material, method, procedure, process, technique, use, equipment, device, apparatus, system, compound, formulation, composition of matter, design or configuration of any kind, or any improvement thereon created or developed by the Receiving Party. You understand that "Inventions" means any and all Inventions that you may solely or jointly author, discover, develop, conceive, or reduce to practice during the period of the contract/ agreement.

   f. Such other information which by its name or the circumstances of its disclosure is confidential. All Confidential Information provided by the Disclosing Party to the Recipient shall remain the sole and exclusive property of the Disclosing Party.

2. The Recipient agrees that at all times it shall: (a) will hold in strict confidence and not disclose to any third party the Confidential Information, except as approved in writing by the Disclosing Party, and (b) will use the Confidential Information only for the Purpose defined in this Agreement; (c) not reproduce Confidential Information in any form except for the Purpose; (d) not use the Confidential Information to make, have made or sell any products or services that compete with any of Disclosing Party's products or services or to exploit commercially and to derive profit and (e) not reverse engineer, decompile, or disassemble any Confidential Information.

3. The Recipient agrees that it shall take adequate measures to protect the secrecy/ confidentiality of and avoid disclosure and unauthorized use of the Confidential Information. The Recipient shall immediately notify the Disclosing Party, in writing, upon discovery of any threatened breach, actual loss, or unauthorized disclosure of the Confidential Information.

4. The Recipient's obligations under this Agreement with respect to any portion of the Confidential Information shall terminate when the Recipient can document that: (a) it was in the public domain at the time it was communicated to the Recipient by the Disclosing Party; (b) it entered the public domain subsequent to the time it was communicated to the Recipient by the Disclosing Party through no fault of the Recipient; (c) it was in the Recipient's possession free of any obligation of confidence at the time it was communicated to the Recipient by the Disclosing Party; (d) it was rightfully communicated to the Recipient free of any obligation of confidence by a third party subsequent to the time it was communicated to the Recipient by the Disclosing Party; (e) it was developed by employees or agents of the Recipient independently of and without use or reference to any Confidential Information communicated to the Recipient by the Disclosing Party; or (f) it is required to disclose pursuant to an order of a duly empowered government agency or a court of competent jurisdiction ,provided due notice and an adequate opportunity to intervene is given to the Disclosing Party , unless such notice is prohibited by such order.

5. Upon completion of the Term of this agreement or upon termination or upon written request of the Disclosing Party, the Recipient shall promptly return to the Disclosing Party all documents and other tangible materials representing the Confidential Information and all copies thereof or certify the destruction thereof.

6. The Parties recognize and agree that nothing contained in this Agreement shall be construed as granting any property rights to the Recipient, by license or otherwise, to any Confidential Information of the Disclosing Party disclosed pursuant to this Agreement, or to any invention or any patent, copyright, trademark, or other intellectual property right in connection therewith. The Recipient shall not derive any profit from the use of-the Confidential Information in an unauthorized manner to the exclusion of the Disclosing Party.

7. The Confidential Information shall not be reproduced in any form except in accordance with the provisions of this Agreement. Any reproduction of any Confidential Information by the Recipient shall remain the property of the Disclosing Party and shall contain any and all confidential or proprietary notices or legends, which appear on the original, unless otherwise authorized in writing by the Disclosing Party.

8. The Recipient acknowledges that its breach of the Agreement may cause irreparable damage to the Disclosing Party and agrees that the Disclosing Party shall be entitled to seek injunctive relief under this Agreement, as well as such further relief as may be granted by a court of competent jurisdiction.

9. The Recipient acknowledges that all documents, including but not limited to any data, analysis, reports, statements, flowcharts, ideas, or any other material prepared by it using the Confidential Information or based on the information provided by GeM is work made for hire ("Work Product"). The Receiving Party shall not use the Work Product for any other purpose or share with a third party without the prior written consent of GeM. Recipient shall be liable for claims against GeM for losses or damages arising out of such unauthorized use or disclosure and shall indemnify and keep indemnified GeM against any such claims.

10. The Agreement contains the final, complete, and exclusive agreement of the Parties relative to the subject matter hereof and supersedes all prior and contemporaneous understandings and agreements relating to this subject matter and may not be changed, modified, amended, or supplemented except by written instrument signed by both Parties. If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such provision shall be severed and the remainder of the Agreement will continue in full force and effect. The Recipient hereby acknowledges that no remedy at law will afford Discloser adequate protection against or appropriate compensation for breach of Recipient's obligations under this Agreement. The Recipient agrees that Discloser shall be entitled to seek specific performance of Recipient's obligations.

11. Recipient will not assign or transfer any rights or obligations under this Agreement without the prior written consent of GeM.

12. This Agreement shall be governed by and construed in accordance with the laws of the India and the Parties hereby submit to the jurisdiction of the courts of New Delhi.

13. Term: This Agreement shall continue in full force and effect for entire Term of the Master Services Agreement ("Term"). The termination of this Agreement shall not relieve the Recipient of its obligations with respect to Confidential Information disclosed under this Agreement. This confidentiality obligation of the Recipient shall prevail over any conflicting term in any other document executed between the Parties, unless otherwise specified.

IN WITNESS WHEREOF, the Parties hereto have caused this Non-Disclosure Agreement to be executed by their duly authorized officers or agents on the date first set out above.

For Government e-Marketplace	For MSP
Authorized Signatory	Authorized Signatory

	For Consortium Partner 1 Authorized Signatory
	For Consortium Partner 2 (if applicable) Authorized Signatory