Open Tender No: STPI/HQ/TECH/DC/CLOS/2022-2023/1

Software Technology Parks of India

REQUEST FOR PROPOSAL (RFP)

FOR

SELECTION OF MSP FOR SETTING UP AND MANAGING GOVERNMENT COMMUNITY CLOUD (GCC)&HYBRID CLOUD IN REVENUE SHARE MODEL

B, office block, STPI, 1st floor, Plate, 1, East Kidwai Nagar, Kidwai
Nagar, New Delhi, Delhi 110023

Disclaimer

The information contained in this Request for Proposal document (the "RFP") or subsequently provided to Bidder(s), whether verbally or in documentary or any other form, by STPI or any of its employees or advisors, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor an invitation by the STPI to the prospective Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their Bid for qualification under this RFP (the "Bid"). This RFP includes statements, which reflect various assumptionsand assessments arrived at by the STPI in relation to the Project. Such assumptions, assessments, and statements do not purport to contain all the information that each applicant may require. This RFP may not be appropriate for all persons, and it is not possible for the STPI, its employees, or its advisors to consider the investment objectives, financial situation and, needs of each party who reads or uses this RFP. The assumptions, assessments, statements, and information contained in this RFP may not be complete, accurate, adequate, or correct. Each applicant should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability, and completeness of the assumptions, assessments, statements, and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Applicant(s) is on a wide range of matters, some of which may depend upon the interpretation of the law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. STPI accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

STPI, its employees, and its advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder, under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment, or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in anyway with pre-qualification of Applicants for participation in the Bidding Process.

STPI also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Applicant upon the statements contained in this RFP. STPI may, in its absolute discretion but without being under any obligation to do so, update, amend, or supplement the information, assessment, or assumptions contained in this RFP.

The issue of this RFP does not imply that STPI is bound to select and pre-qualify bids at the bid stage or to appoint the selected Bidder for the project and STPI reserves the right to reject all or any of the bids without assigning any reasons whatsoever.

The applicant shall bear all its costs associated with or relating to the preparation and submission of its bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by STPI, or any other costs incurred in connection with or relating to its bid. All such costs and expenses will remain with the applicant and STPI shall not be liable in any manner whatsoever for the same or any other costs or other expenses incurred by an applicant in preparation or submission of the bid, regardless of the conduct or outcome of the bidding process.

Glossary

Sr. No	Acronym	Description
1.	AMC	Annual Maintenance Contract
2.	API	Application Programming Interface
3.	BG	Bank Guarantee
4.	CA	Chartered Accountant
5.	CAPEX	Capital Expenditure
6.	CSP	Cloud Service Provider
7.	CV	Curriculum Vitae
8.	DB	Database
9.	DC	Data Centre
10.	DR	Data Recovery
11.	DDOS	Distributed Denial-of-Service
12.	DNS	Domain Name System
13.	ECS	Electronic Clearance Service
14.	EMD	Earnest Money Deposit
15.	FAT	Final Acceptance Test
16.	FS	Final Score
17.	GCC	Government Community Cloud
18.	GoI	Government of India
19.	GST	Goods and Service Tax
20.	GUI	Graphical User Interface
21.	HDD	Hard Disk Drives
22.	ICT	Information and Communication Technology
23.	IaaS	Infrastructure as a Service
24.	INR	Indian Rupees

Sr. No	Acronym	Description
25.	IP	Internet Protocol
26.	ISO	International Organization for Standardization
27.	IT	Information Technology
28.	ITeS	Information Technology Enabled Services
29.	ITSM	Information Technology Service Management
30.	KMS	Key Management Service
31.	KPI	Key Performance Indicator
32.	KYC	Know Your Client
33.	LAN	Local Area Network
34.	MeitY	Ministry of Electronics & Information Technology
35.	MFA	Multi-Factor Authentication
36.	MOU	Memorandum of Understanding
37.	MPLS	Multi-Protocol Label Switching
38.	MSME	Ministry of Micro, Small & Medium Enterprises
39.	MSP	Managed Service Provider
40.	NEFT	National Electronic Funds Transfer
41.	NFS	Network File System
42.	STPI	Software Technology Park of India
43.	NOC	Network Operations Centre
44.	NTP	Network Time Protocol
45.	OEM	Original Equipment Manufacturer
46.	OS	Operating System
47.	PaaS	Platform as a Service
48.	PAN	Permanent Account Number

Sr. No	Acronym	Description
49.	PBG	Performance Bank Guarantee
50.	PC	Personal Computer
51.	PMO	Project Management Office
52.	PoC	Proof of Concept
53.	PSU	Public Sector Undertaking
54.	QCBS	Quality cum Cost-Based Selection
55.	RAM	Random Access Memory
56.	RFP	Request for Proposal
57.	RTI	Right to Information Act
58.	RTO	Recovery Time Objective
59.	RPO	Recovery Point Objective
60.	RCA	Root Cause Analysis
61.	SaaS	Software as a Service
62.	SIEM	Security Information and Event Management
63.	SLA	Service Level Agreement
64.	SOC	Security Operations Centre
65.	SQL	Structured Query Language
66.	SSO	Single Sign-On
67.	STQC	Standardization Testing and Quality Certification
68.	TCP	Transmission Control Protocol
69.	TEC	Tender Evaluation Committee
70.	TRA	Telecommunications Regulatory Authority
71.	UAT	User Acceptance Test
72.	UPS	Uninterrupted Power Supply

Sr. No	Acronym	Description
73.	VM	Virtual Machine
74.	VPN	Virtual Private Network
75.	WAF	Web Application Firewall
76.	WAN	Wide Area Network
77.	R&D	Research and Development
78.	RPA	Robotics Process Automation
79.	AI	Artificial Intelligence
80.	ML	Machine Learning
81.	ACES	Autonomous Connected Electric & Shared
82.	ESDM	Electronics System Design & Manufacturing
83.	STI	Science, Technology & Innovation
84.	NPSP	National Policy on Software Products
85.	NTP	Network Time Protocol
86.	NGIS	Next Generation Incubation Scheme
87.	NCIIPC.	National Critical Information Infrastructure Protection Centre

Definitions

#	Term	Definition
1.	Auditor	Auditor shall mean the Statutory Auditor of a company/ bidder.
2.	Authority	The term "authority" here typically refers to STPI who has the power or right to make decisions or take actions related to this RFP or complete Project.
3.	Authorized Signatory	"Authorized signatory" or signer is a person who's been given the right to sign documents on behalf of the authorizing organization.
4.	Availability	This means the time for which the services and facilities are available for conducting operations on the System including application and associated infrastructure. Availability is defined as: {(Scheduled Operation Time – System Downtime)/ (Scheduled Operation time)} * 100%
5.	Bidder/ Agencies	The "Bidder / Agencies" shall mean the Organization on whose behalf the tender response has been submitted and the bid to perform the Contract has been accepted by the Purchaser and is named as such in the Contract Agreement
6.	Bid / RFP / Tender	This refers to the bid process conducted by STPI, and the technical bid submitted by the successful Bidder, along with the subsequent clarifications and undertakings, if any for the "Selection of MSP for Setting up and Managing Government Community Cloud (GCC) and Hybrid Cloud "the words have been used interchangeably.
7.	Business Day	"Business Day" means any day that is not a Sunday, or a Holiday declared by STPI and/or Government of India
8.	Confidential information	"Confidential Information" means any information disclosed to or by any Party to this Contract and includes any information in relation to the Parties, a third party, or any information including any such information that may come to the knowledge of the Parties hereto / MSP by virtue of this Contract that is by its nature confidential or by the circumstances in which it is disclosed confidential; or is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is or becomes public knowledge other than by a breach of this
9.	Contract/ Master Service Agreement (MSA)	"Contract" means the Tender and all Annexes thereto, the Agreement entered between the selected STPI together with the Purchaser as recorded in the Contract form signed by the Purchaser and the STPI including all Annexures thereto and the agreed terms as set out in the bid, all documents incorporated by reference therein and amendments and modifications to the above from time to time.

#	Term	Definition
10.	CSP	The "CSP" (Cloud Service Providers) means the partner agency to whom the "Bidder" will partner to provide certain specific Cloud services under this RFP.
11.	DC and DR	DC and DR terms are used in this RFP, to denote the proposed Data Centre and respective Disaster Recovery locations, or vice versa, depending upon which site is "primary" for a customer/tenant and which site is "secondary" for the customer/tenant.
12.	Document	"Document" means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes, or databases or microfilm.
13.	Effective Date	"Effective Date" means the date on which this Contract comes into force. This Contract shall come into force and effect on the date (the "Effective Date") of the Purchaser's notice to the MSP Instructing to begin carrying out the activities.
14.	MSP	The "MSP" (Managed Service Provider) shall mean the company/ organization selected by Purchaser because of the tendering process described in this tender document to provide Cloud-related services.
15.	Net worth (Consolidated)	As defined in the Indian companies act 2013
16.	NCIIPC	It is an organization based in India that is responsible for protecting the critical information infrastructure of the country. The NCIIPC operates under the aegis of the Indian government's Ministry of Electronics and Information Technology (MeitY).
17.	Parties	"Parties" means the Purchaser and the successful bidder whereas "Party" means either of the Parties.
18.	Project	"Project" refers to the complete lifecycle from publishing, evaluation, clarification, onboarding, and all activities throughout the contract period including implementation and Management against the RFP; "Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model".
19.	Purchaser	The "Purchaser" shall mean the STPI SI, and its successors and assignees and shall be the agency that shall execute the Project.
20.	Services	"Services" means services to be provided as per the requirements/conditions specified in this tender / contract. In addition to this, the definition would also include other

#	Term	Definition
		related/ancillary services that may be required to execute the Scope of work under the Contract.
21.	Turnover	As defined in the Indian companies act 2013 and its revisions
22.	TEC	A tender evaluation committee is a group or panel tasked with assessing and evaluating the pre-qualification, technical ,and commercial aspects of proposals or bids.
23.	MSP / Successful Bidder	"MSP / Successful Bidder" means the Bidder to whom the "Contract" has been awarded for providing Services as specified in this RFP, Corrigendum, and "Master Service Agreement" and shall be deemed to include the Bidder's successors, subcontractor, representatives (approved by the Department), their, executors, and administrators and permitted assigns unless excluded by the terms of the Contract. MSP / Successful Bidder must abide by all the terms and conditions stated in this RFP, Corrigendum, and Master Service Agreement.
24.	Business Hours	Business Hours of STPI is 09:00 h to 17:30 h
25.	Business Days:	All Working Days, excluding (Saturdays and Sundays) and holidays as identified by STPI. Support Centre is operational on 24 x 7
26.	Scheduled Maintenance Time	Shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. Scheduled maintenance time is planned downtime taken after permission of STPI. Scheduled maintenance time shall be intimated to STPI at least 3 working days in advance.
27.	Scheduled operation time	This means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications will be 24X7X365 (per year).
28.	System or Application downtime	This means the accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the scheduled maintenance time and measured from the time a call is logged with the MSP of the failure or the failure is known to the MSP from the availability measurement tools to the time when the System is returned to proper operation
29.	Steering Committee	Steering Committee is a governing body consisting of members from STPI as well as the selected MSP responsible for

#	Term	Definition
		overseeing and guiding the activities and decision-making related to the data Centre's operations.
30.	Core Committee	STPI will form a Core Committee consisting of STPI officials for overall project governance and monitoring.
31.	Helpdesk Support	Shall mean the support centre which shall handle Fault reporting, Trouble Ticketing, and related inquiries during this contract
32.	Incident	Refers to any event/abnormalities in the functioning of the any of IT Equipment/Services that may lead to disruption in normal operations of the IT infrastructure, Cyber Security infrastructure, or Application services

Table of Contents

Section I: Invitation to Bid

Open Tender No. STPI/HQ/TECH/DC/CLOS/2022-2023/1

Software Technology Parks of India

B, office block, STPI, 1st floor, Plate, 1, East Kidwai Nagar,
Kidwai Nagar, New Delhi, Delhi 110023

STPI invites online bids (Technical & Commercial) from eligible bidders which shall be valid for a minimum period of 180 days from the date of bid submission for “RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model”.

Scope of Work	RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model	
EMD to be submitted	INR 1,00,00,000/- (Rupees One Core Only)	Earnest Money Deposit (EMD) submitted in the form of a Bank Guarantee/demand draft / electronic transfer B.1)
Last date and time of uploading of Bids		26.06.2023, 17:00 Hrs
Date and time of opening of Technical Bids		28.06.2023, 17:30 Hrs.

Note: In case of EMD submitted in the form of BG then original BG should be submitted at STPI office before Bid Submission.

CAO-cum-Registrar
STPI

Tel. 011-24628081 /24346600

Email: cloudrfp@stpi.in

FACTSHEET

#	Information	Details
1	Tender No	STPI/HQ/TECH/DC/CLOS/2022-2023/1
2	Project Name/ Name of Work	Selection of MSP for setting up Hybrid Cloud and GCC cloud and managing the revenue sharing model
3	Tender Type	Open
4	Tender Category	Services
5	Submission Mode & Website to download	Online through https://eprocure.gov.in/eprocure/app
6	Date of Publishing the RFP	25.05.2023
7	Bid submission start date	25.05.2023
8	Document download start date	25.05.2023
9	Document Download end date	23.06.2023
10	Last date & time for submission of Pre-Bid Queries	05.06.2023, 15:00 Hrs
11	Pre-Bid Meeting	09.06.2023, 15:00 hrs https://stpi.webex.com/stpi/j.php?MTID=md50338eeca10ec77615da9a5210036c8 Friday, June 9, 2023 3:00 PM | 2 hours | (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi Meeting number: 2524 640 8552 Password: WJmAsdna336 Join by video system Dial 25246408552@stpi.webex.com You can also dial 210.4.202.4 and enter your meeting number.
12	Last date and time (deadline) for uploading the bid on the e-Tendering website	26.06.2023, 17:00 Hrs
13	Date and time of Opening of the Bid	28.06.2023, 17:30 Hrs
14	Date of Opening of Commercial Bids	To be declared later
15	Presentation by Bidders	To be declared later
16	Tender Fee	Nil
17	Earnest Money Deposit (EMD)	INR 100,00,000/- (Rupees One Crore Only) valid during the Bid Validity Period and additional 30 days post Bid Validity Period
18	Bid validity period	180 Days from the last date of submission of Bids
19	Validity of This Contract	123 Months
20	Number of Covers/Packets/Envelop	Packet 1: Technical Bid (Pre-qualification & Technical Qualification) Packet 2: Commercial Bid

#	Information	Details
21	Contact Details	1st Floor, Plate B, Office Block - 1, East Kidwai Nagar, New Delhi 110023 Email: cloudrfp@stpi.in Ph: 011-24628081 /24346600
22	Bank Account Details of STPI	Canara Bank Delhi Parliament Street Branch New Delhi. 110002 Account No: 1098101101244 IFSC: CNRB0001098

1.1 About STPI

Software Technology Parks of India (STPI) is a premier S&T organization under Ministry of Electronics and Information Technology (MeitY) engaged in promoting IT/ITES Industry, innovation, R&D, start-ups, product/IP creation in the field of emerging technologies like IoT, Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Computer Vision, Robotics, Robotics Process Automation (RPA), Augmented & Virtual Reality, Animation & Visual effect, Data Science & Analytics for various domains like Gaming, FinTech, Agritech, MedTech, Autonomous Connected Electric & Shared(ACES) Mobility, ESDM, Cyber Security, Industry 4.0, Drone, Efficiency Augmentation, etc.

Since its inception in 1991, STPI has been working towards equitable and inclusive IT-led growth pan-India which in turn has helped promoting Software exports, Science, Technology & Innovation (STI) and Software product development. With ten jurisdictional directorates and 63 centres, STPI has expanded its presence pan-India to support IT/ITeS Industry. Working closely with all stakeholders, STPI has played a key role in transforming the country as the preferred IT destination, a fact that aptly proven by the stupendous growth in exports by STPI-registered units from Rs. 52 crores in 1992-93 to Rs. 7.4 lakhs crores in 2022-23.

STPI is aspiring to become the largest technology start-up ecosystem in the country and has been endeavouring to transform the country into a software product nation as envisaged in National Policy on Software Products (NPSP) 2019. To achieve this, STPI has evolved a collaborative model wherein government, industry, academia, and other stakeholders are playing a vital role for providing end-to-end support to start-ups. Aligned with this vision for promoting R&D, innovation, product & IPR creation, STPI is providing state-of-the-art infrastructure, skilling, mentoring, market connect and other necessary support pan-India to start-ups. STPI has also embarked on launching Next Generation Incubation Scheme (NGIS), a futuristic incubation scheme to offer comprehensive support & services and extend seed funding to start-ups from 12 STPI incubation facilities pan-India at Agartala, Bhilai, Bhopal, Bhubaneswar, Dehradun, Guwahati, Jaipur, Lucknow, Mohali, Patna & Vijayawada under a common umbrella. To further strengthen the start-up ecosystem in the country, STPI has set up RF Lab, EV Lab, AV Lab, IoT Lab, MoCap Lab, AI/DA Lab, Innov IoT Lab, CV/AI Lab, ESDM Lab, Health Informatics Lab, MediElectronics Lab, VR/AR Lab, Fintech SandBox, FabLab, SMARTLab, and Atal Incubation Centre (AIC) to enable start-ups leverage these facilities for building innovative technology products and solutions in an indigenous manner.

1.2 STPI Data Centre Locations

STPI has expanded its presence pan-India since its inception in 1991 with 3 centres to promote and disperse the IT/ITES industry. Today, STPI has 63 centres of which 55 centres are in Tier-II/III cities. The details of the existing Tier III Data Centres of STPI are provided as following:

Data Centre Details	Bengaluru*	Bhubaneswar	Mohali*	Chennai	Vijayawada
Address	No.76,77 & 78(p) 1st Floor, Keonics Electronics City Phase-1 Hosur Main Road Bengaluru-560100 Karnataka	STPI, Elite Building, Idco Plot No 2/A, Gothapata Na, Malipada, Bhubaneswar, Khordha-751003 Orissa	Plot C-184, Phase-8A, Industrial Area, Sector- 75 Mohali Punjab	No.5, Rajiv Gandhi Salai, Tiramani, Chennai, 600113. Tamil Nadu	Vincity Building, Near Polytechnic College, Patama, Vijayawada, AP 520008

Data Centre Details	**Bengaluru***	**Bhubaneswar**	**Mohali***	**Chennai**	**Vijayawada**
Date Commissioned	01.04.2020	31.10.2020	01.04.2017	15.07.2009	01.05.2019
Total Incoming Power to Land	2.5 MVA	1.25 MVA	2.5 MVA	1.6 MVA	440 KVA
Total Incoming Power to Data	1.6 MVA	820 KVA	800 KVA	0.7 MVA	250 KVA
Total Area of the Building	19320 sq. ft.	78442 sq. ft.	145713 sq. ft.	11463 sq. ft.	50000 sq. ft.
Total Area of IT/Computer Room Space	15570 sq. ft.	3380 sq. ft.	14482 sq. ft.	3500 sq. ft.	2452 sq. ft.
Design Capacity	1.6 MW	0.82 MVA	2.5 MVA	0.7 MW	450KVA
Available Capacity	1 MW	0.82 MVA	2.5 MVA	0.3 MW	450KVA
Target Tier (I-IV)	Rated III (Certified)	Tier III (Compliant)	Tier-III (Compliant)	Tier III (Compliant)	Tier-III (Compliant)
Target PUE	1.8	1.8	1.7	1.85	1.8
UPS Configuration (e.g., N+1, 2N)	N+N	N+N	N+N	N+N	N+N
Industry or Compliance Certifications	ISO 9000,20000,27001	ISO 27001:2013 is under process	GRIHA 5 Star and ISO 27001:2013	ISO 9000, 20000,27001	ISO 9001:2015, ISO 27001:2013
Total number of Racks (Commissioned)	165	49	120	74	10
Total number of Racks (Expansion space)	40	72	40	26	10

***Note: STPI's Mohali and Bangalore Data centre locations are being operated and managed by a third-party vendor on PPP model currently**

1.3 STPI Edge Location Data Centres

Apart from Tier-III compliant Data Centres, STPI has around 50+ Tier-II level Data Centre/NOC infrastructure (primarily being utilised as ISP Point of Presence (POP)) at the following locations.

State	Location
Andhra-Telangana	Hyderabad - ses (jubilee hills) (NoC)
	Hyderabad - solitaire building (NoC)
	Warangal (NoC)
	Vijayawada (NoC)
	Visakhapatnam (NoC)
	Tirupati (NoC)
	Kakinada (NoC)
Tamil Nadu	MSITS data centre Chennai (NoC)
	Chennai (NoC)
	Pondicherry (NoC)
	Trichy (NoC)
	Coimbatore (NoC)
	Madurai (NoC)
Karnataka	Bengaluru
	Mangalore
	Hubballi
	Davanagere
	Mysuru
Gujarat	Gandhinagar
	Surat
Kerala	Thiruvananthapuram
	Kochi
West Bengal	Kolkata
	Durgapur
	Kharagpur
	Siliguri
	Haldia
Northeast India	Guwahati
	Shillong
	Gangtok
	Agartala

State	Location
	Aizawl
	Imphal
	Kohima
	Itanagar
Maharashtra	Mumbai
	Pune
	Nagpur
	Nashik
	Kolhapur
UP, MP, Chhattisgarh, Uttarakhand	Lucknow
	Kanpur
	Prayagraj
	Bhopal
	Indore
	Bhilai
	Meerut
	Dehradun (Sub Centre)
	Dehradun
	Gwalior
	Noida
Haryana	Gurugram
Rajasthan	Jaipur
Goa	Goa
Himachal Pradesh	Shimla
Punjab	Mohali
Jammu & Kashmir	Srinagar

Section II: Instruction to Bidders

2.1. Purpose of RFP

STPI intends to issue this bid document, to eligible entities, to participate in the competitive bidding for the “RFP for Selection of MSP for “Setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model”. For this purpose, STPI invite proposals for onboarding MSP & CSP to undertake the activities as mentioned under **“Scope of Work”**, the proposed services should be managed with SLA driven, Scalable, Extensible, Highly Configurable, Secure and Responsive way in the best possible revenue sharing model. The broad objective of the RFP is provided as following:

1. Setting up and managing Government Community Cloud (GCC) & Hybrid Cloud at existing STPI Data Centres.
2. Establishing STPI as a leading MeitY empanelled Cloud Service Provider.
3. To provide a complete IT platform with agility and reliability via advanced cloud services (IaaS, PaaS, SaaS) to Start-ups, Enterprises and Govt. departments.
4. To facilitate the Start-up ecosystem by hosting digital products on the STPI platform at single marketplace.
5. Leveraging the Edge DC locations of STPI for providing applicable cloud services.
6. Public & Private Partnership (Revenue sharing) to capitalize on the industry expertise.
7. Generate maximum revenue per KW/per sq. feet by providing bouquet of cloud services from the existing Data Centre facilities.
8. To establish STPI as a leading player for Cloud services to serve Indian and offshore clients.

The Managed Service Provider (MSP) shall offer advanced Hybrid cloud services (IaaS, PaaS, SaaS) from existing STPI Data Centres, which may be extended to the new facilities as they are ready in future.

2.2. Instructions for online bid submission

a) Proposals must be direct, concise, complete and must primarily be submitted online only on the CPP portal. STPI will evaluate Bidder’s proposals based on their clarity, relevance, and timeliness to the program requirements set out in this RFP.

b) Bidders shall provide the required information on their technical and commercial offers only as per the formats provided in the RFP. Any deviations in the format will make the offer liable for rejection.

c) The following points should be considered while bidding: -

   i. Tender notices/routine communications will be uploaded/issued on the website https://eprocure.gov.in/eprocure/app, the Central Public procurement portal.

   ii. All the bids (Technical as well as Commercial) shall have to be submitted online.

   iii. The date and time for online submission will be communicated on the e-tendering website. Bidders should ensure their bid should be submitted online before the scheduled date and time. No delay for any reason will be accepted. Bids not submitted online shall not be considered.

   iv. STPI may, at its own discretion, extend the date for the bid submission. In such a case, all rights and obligations of the STPI and the bidders shall apply to the extended time frame.

   v. Bids submitted as documents by telex/telegram/fax/e-mail or by other means not specified in the RFP will not be considered. No correspondence will be entertained on this matter.

vi. Bidders printed terms and conditions will not be considered part of their bid.

vii. Any further changes to the RFP will be communicated to the bidders through the website https://eprocure.gov.in/eprocure/app. Bidders should take these changes into account when preparing their bids.

viii. As such, STPI will bear full power to withdraw the tender at any stage without prior intimation to the bidders.

2.3. Clarification on Tender Document

A prospective Bidder requiring any clarification on the tender document may submit his queries in writing, at the STPI's mailing address viz; cloudrfp@stpi.in as per schedule indicated in the RFP document. The queries must be submitted in the following format (explicitly in MS word/MS Excel file, *.xls/xlss) only to be considered for clarification:

Sr. No	Section No.	Clause No.	Reference/ Subject	Clarification Sought
..	..	..	..	..

STPI may not respond to any queries not adhering to the above-mentioned format.

Note: Inputs/suggestions/queries submitted by the bidders as part of the pre-bid meeting and otherwise will be given due consideration by STPI. However, STPI is not mandated to accept any submission made by the bidders.

2.4. Procedure of submission of bid

a) To view Tender Notice, detailed time schedule of this tender, please visit the following e-Tendering website: https://eprocure.gov.in/eprocure/app.

b) Bidders participating in the eProcurement portal for the first time will need to complete the online registration process for the e-Tendering portal.

c) Bidder is expected to review all instructions, forms, conditions, project requirements, and other information in the RFP documents. Failure to provide all the required information set forth in the RFP documents or to submit a proposal that does not substantially confirm the RFP documents in any respect shall be at the Bidder's risk and may result in rejection of the proposal.

2.5. Two Packet Bid System

Complete bidding process will be online (e-Tendering) in **two packet** system. Submission of bids shall be in accordance with the instructions given below:

A. Packet 1: Pre-Qualification and Technical Proposal - Bidder should upload information as scanned copies in PDF format as required in the RFP.

(i) **Pre-Qualification** - The requirements for submission of the Pre-qualification Bid is provided in the RFP document.

(ii) **Technical Bid** – The format for submission of the Technical Bid is provided in the RFP document.

B. Packet 2: Commercial Proposal – Bidder should provide as per "Commercial Bid Format" of this RFP.

The packets to be submitted by the bidder shall consist of following minimum documents in accordance with the instructions given below:

Packet 1 (Pre-Qualification and Technical Proposal)	1. Proof of submission of EMD should be submitted as part of the Pre-qualification Proposal. 2. Bidder’s response to the Pre-Qualification criteria defined in the RFP shall be submitted as marked “Pre-Qualification Proposal”. 3. The Pre-qualification related documentation shall be prepared in accordance with the requirements specified in this RFP and in the formats prescribed in the RFP document. 4. Duly signed Integrity Pact. 5. Pre-Qualification Proposal should not contain commercials of the Project, in either explicit or implicit form. 6. Certified true copy of a board resolution/power of attorney empowering authorized signatory to sign/act/execute documents binding the bidder organization to the terms and conditions detailed in this proposal. 7. The Technical Proposal shall be prepared in accordance with the requirements specified in this RFP and in the formats prescribed in the RFP document. 8. Duly filled technical specification with cross reference details. 9. Technical Proposal should not contain commercials of the project, in either explicit or implicit form. 10. The Bidder may be required to give a presentation on their Proposal. STPI will suggest the timing and venue of the presentation(s). 11. Any information obtained during the presentation and/or visit will not be deemed to change or supplement the Bidder’s Proposal as set out in the RFP. 12. Conditional technical proposal is liable for rejection. **Note**: All documents will be submitted in pdf format and uploaded in the central public procurement portal.
Packet 2 (Commercial Proposal)	1. Commercial details (in the format given in the RFP) shall be submitted online in a separate Packet marked “Commercial Proposal” to be submitted as (xls/xlss format) – Annexure-J on the central public procurement portal. 2. Forms and formats mentioned in this RFP document need to be scrupulously followed. Any deviation in it (without proper justification) may lead to disqualification of the bid. 3. Bid quotation accompanied by vague and conditional expressions such as "subject to immediate acceptance", "subject to confirmation", etc. will be treated as being at variance and shall be liable to be summarily rejected.

Note: If commercial bid is provided with technical bid in same packet, then the bidder will be disqualified.

STPI will not accept submission of the commercial proposal in any manner other than that specified in the RFP Document. Proposals submitted in any other manner shall be treated as defective, invalid, and rejected.

Packet 1 (Pre-Qualification & Technical Proposals) and Packet 2 (Commercial proposals) should be signed by an authorized person of the bidder. The Pre-qualification proposal should be submitted along with a certified true copy of a board resolution/power of attorney empowering authorized signatory to sign/act/execute documents binding the bidder organization to the terms and conditions detailed in this proposal. Proposals must be direct, concise, and complete. STPI will evaluate bidder’s proposal based on the clarity and completeness of its response to the requirements of the project as outlined in this RFP.

2.6. Bid validity period

Bids should remain valid for a period of 180 days from the last date of bid submission.

2.7. Bid Opening

a) STPI will convene a bid opening session as specified in FACTSHEET, which may be attended by one representative of the bidder organization who has successfully uploaded the bid.

b) STPI will first download the Packet-1 from the e-tender portal. Bidder representative may remain present during the bid download process.

c) The bids will then be passed to a duly constituted Tender Evaluation Committee (TEC). The Commercial bids of only those bidders whose bids are found qualified by the evaluation committee as per both pre-qualification and technical qualification criteria will be opened in the presence of the bidder's representatives subsequently for further evaluation.

2.8. Withdrawal, Modification or Correction of Bids

No bid may be modified, corrected, or withdrawn after the closing date prescribed in the RFP.

2.9. Rejection of Bid

STPI reserves the right to reject a proposal/bid on the following grounds:

2.9.1. General Rejection Criteria

a) If a commercial bid is provided with the technical bid in the same packet, then the bidder will be disqualified.

b) In case of offers with incomplete information, offers that are subjective and conditional, and offers that are partial.

c) Proposals submitted without attachments to support the applicant's specific experience in relevant projects, proposed work plan, approach and methodology and CVs of experts to be deployed.

d) Proposals with variation/contradiction between pre-qualification offer, technical offer, and commercial offer.

e) Proposal without a signed copy of the proposal and all relevant documents.

f) In addition to the above criteria, if any of the provisions of this RFP are not followed, the proposals may be rejected.

Failure to comply with the terms & conditions.

2.9.2. Technical Rejection Criteria

a) Non-compliance: The proposal fails to comply with the stated requirements, specifications, or standards outlined in the RFP document.

b) Lack of Technical Feasibility: The proposal demonstrates a lack of technical feasibility to successfully implement the project or fulfil the specified objectives.

c) Substandard Quality: The proposal does not meet the expected quality standards as defined in the RFP, including but not limited to performance, durability, reliability, and safety.

d) Inadequate Expertise: The proposing entity does not possess the necessary technical expertise, qualifications, or experience required to undertake the project.

e) Failure to Provide Sufficient Documentation: The proposal lacks essential technical documentation, such as asked technical proposal details, detailed technical specifications with asked references, test plans, or relevant information/certifications, which are necessary for a comprehensive evaluation.

f) Non-Conformance with Legal or Regulatory Requirements: The proposal violates applicable laws, regulations, industry standards rendering it non-compliant and unsuitable for further consideration.

2.9.3. Commercial Rejection Criteria

a) Non-Conformance with Terms and Conditions: The bid fails to meet or comply with the specified terms, conditions, or contractual requirements outlined in the RFP document, including but not limited to delivery schedules, payment terms, warranties, or other commercial provisions.

b) Inadequate Financial Stability: The bidding entity lacks the necessary financial stability, solvency, or creditworthiness to fulfil the contractual obligations or provide the required goods/services for the duration of the project.

c) Insufficient Capacity or Resources: The bidding entity does not possess the requisite capacity, resources, or infrastructure to effectively carry out the project, meet the specified volume or demand, or ensure timely completion.

d) Non-Responsiveness: The bid fails to address all the requirements stated in the RFP or lacks essential information/documentation necessary for evaluation, making it incomplete, ambiguous, or non-responsive.

e) Conflict of Interest: The bidding entity has a conflict of interest that could compromise the fairness, transparency, or integrity of the procurement process or raise concerns regarding undue influence, bias, or impropriety.

2.10. Clarification of Bids by STPI

a) During the bid review, STPI may seek clarification on the bids. Detailed procedure for such clarification may be provided to the Bidder after receipt of the bid as deemed appropriate.

b) The Bidder shall provide full and comprehensive responses of clarification requests.

c) STPI reserves the right to request additional information/documents from the bidder to obtain clarification. These additional documents must be submitted within the specified timeframe. Failure to provide the requested documents within the given timeframe may result in the bid being rejected.

d) Any information discussed during meetings will be recorded including records of clarifications requests related to the RFP and replies of such requests.

2.11. Language of the Bid

The Bids prepared by the Bidder and all subsequent correspondence and documents relating to the bids exchanged by the Bidder and STPI, shall be written in English language. Any printed literature furnished by the Bidder, written in another language, shall be accompanied by an accurate English translation, for purposes of interpretation of the bid.

2.12. Earnest Money Deposit (EMD)

The bidder is requested to provide an Earnest Money Deposit (EMD) of a sum equivalent to INR 1,00,00,000/- (Rupees One Crore Only) as a demonstration of their serious intent and commitment to participate in this Request for Proposal (RFP) process. The EMD shall be in the form of bank Guarantee/demand draft / electronic transfer, payable to STPI. The format for EMD is provided as per Annexure-B.1. Bidders may note that:

I. A proposal that is not accompanied by the EMD will be summarily rejected.

II. STPI is not obliged to pay any interest on the EMD.

III. In the event of any discrepancy or disagreement regarding the forfeiture or release of the EMD, the decision of STPI shall be final and binding.

IV. Upon the successful award of the contract, the EMD shall be returned to the successful bidder after 30 days of submission of Performance Bank Guarantee (PBG)

V. The EMD may be forfeited:

a. If the bid is withdrawn during the validity period or any extension thereof agreed to by the bidder.

b. If the successful bidder fails to execute the contract or defaults on any of its obligations.

c. If the successful bidder fails to sign the contract and submit Performance Bank Guarantee within the stipulated period.

d. If the bid is varied or modified in a manner not acceptable to STPI after opening of the bid during the validity period or any extension thereof.

VI. If the Bidder attempts to influence the evaluation process.

VII. EMD is to be submitted along with the bid by the bidders. Therefore, the last date of submission of EMD will be the same as last date of submission of the bids.

In addition to the above as per Rule 170 of GFR-- “Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Ministry of Micro, Small and Medium Enterprises (MSME)” are exempt from submission of EMD (Bid security). Bidders claiming exemption of EMD under this rule(170 of GFR) are however required to submit a signed Bid securing declaration refer to **(Annexure B.2**) accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they may be blacklisted or face legal consequences.

2.13. Performance Bank Guarantee (PBG)

a. For the performance of its obligations, the successful bidder shall ensure the submission of an irrevocable and unconditional Bank Guarantee of a sum equivalent to INR 2,00,00,000 (Rupees Two Crore Only), no later than 30 (thirty) days from the date of signing the contract. The format for PBG is specified as per **Annexure-C** of this RFP. The PBG shall be valid for a term of the resultant Agreement and shall be renewed and maintained as necessary by the MSP for the term of the resultant agreement, and extensions if any.

b. Until such time the Performance Security for year 1 (one) is provided by the MSP, the EMD shall remain in force and effect, and upon such provision of the Performance Bank Guarantee pursuant hereto, the STPI shall release the EMD to the MSP.

c. The Performance Bank Guarantee shall remain valid until the MSP has fully completed all obligations under the contract. However, after two years of the contract award, the Performance Bank Guarantee shall be revised by the MSP. The revised value will be either 3% of the total revenue earned by the MSP in the previous financial year or INR 2,00,00,000 (Rupees Two Crore Only) whichever is higher. Further, the PBG shall be revised on the interval of every two-year considering above criteria till the end of the contract period.

d. The Performance Bank Guarantee shall be obtained in compliance with Applicable Laws (including, in case the MSP is a non-resident, in compliance with applicable foreign exchange laws and regulations).

e. The Performance Bank Guarantee is to be apportioned against breach of this Agreement by the MSP or for recovery of liquidated damages as specified in the **Section 3.17.12.** In any of the foregoing events, STPI shall, without prejudice to its other rights and remedies hereunder or in law, be entitled to encash and appropriate from the PBG, the amounts due to it. Upon such encashment and appropriation from the Performance Security, the MSP shall, within 15 (fifteen) days thereof, replenish, in case of partial appropriation, to its original level the Performance Security, and in case of appropriation of the entire Performance Security, provide a fresh Performance Security, as the case may be, and the MSP shall, within the time so granted, replenish or furnish fresh Performance Security as aforesaid, failing which the Authority shall be entitled to terminate this Agreement in accordance with **Section 3.15.**

f. The Performance Bank Guarantee shall remain in force and effect during the entire term of the contract agreement, and shall be released thereafter; provided, however, the Performance

Security shall not be released if the MSP is in breach of the Contract Agreement. After the expiry/termination of the agreement, STPI shall return/release the Performance Security, after applicable deductions as per the contract Agreement, if any.

g. The PBG shall be forfeited by STPI, in case:
   i. The MSP does not meet the overall condition stated in this RFP or any changes agreed between the parties.
   ii. MSP do not fulfil the duties and obligations set forth in the RFP to the satisfaction of STPI.
   iii. Misrepresents facts/information submitted by MSP to STPI.

2.14. Bid Prices

The bidder shall prepare the bid based on details provided in the tender documents. It must be clearly understood that the Scope of Work is intended to give the bidders an idea about the order and magnitude of the work and is not in any way exhaustive and guaranteed. The bidder shall carry out all the tasks in accordance with the requirement of the tender documents & with due diligence. It shall be the responsibility of the bidder to fully meet all the requirements of the tender documents and to meet objectives of the project. If during execution of the project, any minor revisions to the work requirements like technical specifications, equipment sizing, etc. are to be made to meet the goals of the project; such changes shall be carried out within the proposed price. If any deviation has a major impact on the commercials, STPI shall take appropriate decision and such decisions would be binding on the MSP.

2.15. Firm revenue share

Revenue percentage share offered by the bidder quoted in the bid must be firm and final and shall not be subject to any downward modifications, on any account whatsoever. STPI reserves the right to negotiate the Revenue percentage share offered by the bidders in the bid considering any extra ordinary market conditions or exigency.

Revenue percentage share offered by the bidders in any form or by any reason before opening the Commercial Bid should not be revealed, failing which the offer shall be liable for rejection. If revenue percentage share offered change is inevitable due to any factor external to the bidder, bidders may be given chance to submit revised bids. In this regard, the decisions of STPI shall be final.

2.16. Amendment of RFP Document

At any time prior to the submission of bids, STPI for any reason whatsoever, may, modify any element of the RFP document by issuing a corrigendum, which shall be notified on CPP portal. For the sake of interpretation, the content of any corrigendum issued by the STPI shall be read as a part of the original bid. In each instance in which provisions of the corrigenda contradict or are inconsistent/ inapplicable with the provisions of the RFP, the provisions of the corrigendum shall prevail and govern, and the contradicted or inconsistent/inapplicable provisions of the RFP shall be deemed amended accordingly. STPI may in its sole discretion consider extension of deadlines for submission of the bids, to allow prospective bidders reasonable time in which to take the amendment into account while preparing their bids.

2.17. Legal Relationship

No binding legal relationship will exist between any of the bidders and STPI until the issues of purchase order / execution of a contractual agreement.

2.18. Signing of Bid

The "Bidder" as used in the RFP documents shall mean the one who has signed the Bids. The Bidder may be either the Constituted attorney of the company or the Principal Officer or his duly Authorized Representative, in which case he/she shall submit a certificate of authority. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall, be furnished and signed by the Bidder.

It is further clarified that the individual signing the Bid or other documents in connection with the Bid must certify whether he/she signs as:

I. Constituted attorney of the company.

OR

II. The Principal Officer or his duly Authorized Representative of the company, in which case he/she shall submit Authorization Letter/Power of Attorney on behalf of the company as per format provided in **Annexure D and F**.

2.19. Duration of the contract

The Contract shall be valid for a period of 123 months from the date of signing of contract. STPI reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the bidder, at least 3 months before the expiration of the term. The decision to grant or refuse the extension shall be at the STPI's discretion. Accordingly, the Performance Bank Guarantee shall be extended up to the extended contract period.

2.20. Renewal/ Extension of contract

1. Upon the successful completion of the initial contract duration of 123 months, STPI reserves the right to renew or extend the contract on a per-year basis, subject to mutual agreement and satisfactory performance criteria.
2. The decision to renew or extend the contract shall be based on the satisfactory performance of the selected MSP throughout the initial contract period, including adherence to agreed-upon service levels, timely deliverables, effective management of resources, and compliance with all contractual obligations.
3. The renewal/extension of the contract shall be subject to negotiation of mutually agreeable terms and conditions between the STPI and the selected MSP.
4. The renewal/extension of the contract shall be for a period of one year, with the option for further renewal/extension for additional one-year period, subject to the terms and conditions to be same as the original contract unless otherwise agreed upon by both parties.

2.21. Qualification Criteria and Evaluation

Bids will be assessed by adopting a three-stage evaluation process as mentioned below:

1. Pre-Qualification Evaluation
2. Technical Evaluation
3. Commercial Evaluation

The Bid responses shall be evaluated for the Pre-qualification criterion first and shall be evaluated further if qualified. All documents provided by the MSP and CSP should be duly signed/counter signed by authorized signatory of the MSP.

Eligibility criteria for bidder MSP and CSP are furnished as below:

2.21.1. MSP Pre-Qualification Criteria

#	Category	Criteria	Documents Required
1	Legal Entity	The MSP must fulfil all the following: a. MSP must be a Legal Entity i.e., a company incorporated in India under the Companies Act, 1956 or 2013 **OR** LLP Act 2008/ Partnership Act, 1932. **OR** A partnership firm registered under Indian LLP act 2008. and subsequent amendments thereto b. Registered with the Income Tax (PAN) and GST (GSTN) Authorities in India with active status c. Should submit last 3 years (2019-20, 2020-21 & 2021-22) IT returns d. Should have at least one permanent office in India	Copy of a. Certificate of incorporation b. CIN c. GST registration certificate d. PAN e. Copy of IT returns f. Office registration certificate or tax receipt. g. Copy of self-declaration stating at least one permanent office in India
2	Financial: Turnover	The MSP must have an average annual revenue from operations of not less than Rs 500 crore for the last three consecutive financial years (2019-20, 2020-21 & 2021-22) from the Data Centre/Cloud-related services/Managed IT Services as of 31.03.2022. **Note:** Turnover from the group companies shall be considered.	Copy of audited Profit and Loss Account, Balance Sheet, Income Tax Returns of the last three financial years and Certificate from statutory auditor/CA quantifying the average annual revenue from Data Centre/ Cloud related/Managed IT services. ***(Refer Form-1, Annexure D)***
3	Financial: Net Worth	The Net worth of the Bidder for each of the three financial years (FY 2019-20, 2020-21 & 2021-22) should be positive.	Statutory Auditor Certificate with Registration Number and Seal ***(Refer Form-2, Annexure D)***

#	Category	Criteria	Documents Required
4	Project Experience	The MSP must have at least two (at least one completed) projects of INR 50 crores (Fifty Crores Rupees) each with scope covering IT implementation of Data Centre Infra during last 3 years as on bid submission date in India. The project should be for own company or for a client. For internal projects, the value to be considered is cost incurred till Go-Live.	The Bidder shall provide: **For External Projects** a. Details of work orders/ Purchase b. Completion certificate Or c. Undertaking mentioning project value and status (in case of ongoing project) **Note**: Certificate to the effect shall have to be provided from the client clearly defining the name, address, contact person, and contact number, email address. ***(Refer Form-3, Annexure D)*** In case of non-Disclosure agreement (NDA) with Client only An undertaking in this regard must be provided by the Statutory Auditor. ***(Refer Form-4, Annexure D)*** ***For Internal Projects*** An undertaking in this regard must be provided by the bidder on its company letter head duly signed and stamped from authorized signatory. Undertaking should clearly specify the scope of work, project start, Go- Live date, current status and total project value including taxes. ***(Refer Form-7, Annexure D)***
5	NoC Experience	MSP should have an operational Public Cloud/private cloud/managed IT services, with a self-service portal, with at least 50 cloud customers for which the bidder has managed NoC operations. The services that bidder has provided must include: 1. Cloud Services 2. Network Management Services MSP should have 24x7x365 NOC operations.	Self-Certificate along with the name, address, contact person, contact no., and email address of the customer.

#	Category	Criteria	Documents Required
7	Manpower	MSP must have at least 150 employees working in the cloud operations/managed IT services. Out of which at least 20+ certified resources on the proposed cloud platform at the time of RFP submission	Certificate from statutory auditor/ Signing Authority (HR head).
8	Certifications	The MSP must possess all three valid latest certifications at the time of submitting the Bid. A. ISO 9001:2015 B. ISO 20000 C. ISO 27001	Copy of Valid Certificate **Note:** If any certificate is not available/is under process, then self- certified declaration by the authorized signatory of the bidder should be submitted along with the proposal and valid certificate is to be submitted at award of contract.
9	Mandatory Undertaking	The bidder shall submit the undertaking that their entity should not be: a. insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons. b. debarred and/ or blacklisted by any organization of GoI/Central PSU/ State Government entities as on the bid submission date. c. and their directors and officers have not been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings	Self-certification by the authorized signatory duly signed and stamped on the company letterhead. ***(Refer Form-8, Annexure D)***
10	IT Act	MSP must be compliant with IT Act 2000 (including 43A) and amendments.	Self-declaration from the Authorized signatory of the bidder on their letterhead. ***(Refer Form-5, Annexure D)***

Note:

The qualification criteria shall be complied by the bidder entity **OR** Parent entity/Group Company/ of bidder entity (provided bidder is subsidiary of the Parent entity) **OR** jointly by bidder entity and parent entity/group company. In case parent entity/group company experience and other details are used, proof of relationship between the bidder and parent entity needs to be submitted duly signed by authorised signatory. (.as per Annexure O)

2.21.2. CSP Pre-Qualification Criteria

#	Category	Criteria	Documents Required
1	Financial: Turnover	The CSP must have an average annual turnover from operations of not less than INR 500 crore (Rupees Five Hundred Crores Only) for the three consecutive financial years (FY 2019-20, 2020-21 and 2021-22) from cloud-related service.	Copy of audited profit and loss account and balance sheet of the three financial years and Certificate from the statutory auditor/CA quantifying the average annual turnover ***(Refer Form-1, Annexure F)***
2	CSP Presence and Services	The CSP should be registered under the Companies Act, 1956 or 2013 or LLP firm/ Partnership firm under Partnership Act 1932 and should be in operation for at least 3 years as of 31.03.2022.	Copy of i. Certificate of incorporation ii. GST registration certificate iii. PAN
3	ISO Certifications	CSP must have all the following valid latest certifications for its facilities in India: (a) ISO 20000 (b) ISO 27001 (c) ISO 27701	Valid Copy of the certificates
4	Data Centre Facility	CSP's Data Centre from where the Public Cloud services will be offered must be operational in India (as of 31 March 2022), with at least 100 operational racks and it must be at least Rated- 3/Tier 3 standard and preferably certified under TIA 942 or uptime or any 3rd party institution certification. The DC Facility must have a) Routers, Firewalls, LAN, WAN, Internet b) Access, Hosting Centres, Backup, Operations Management, and Data Management Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)	a. Valid Copy of uptime/TIA 942 certificate b. Confirmation from the bidder on Tier-III/Rated 3 standards declaration ***(Refer Form-2, Annexure F)***
5	Accreditations	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity,	Copy of SOC1, SOC2 and SOC3 Certificates / Reports

#	Category	Criteria	Documents Required
		and/or privacy Trust Services principles.	
6	Financially Backed SLA	The CSP should provide financially backed SLAs for all the services offered on Public Cloud and these SLAs should be declared in public portal of CSP.	a. CSP Self-Declaration from the authorized signatory. b. URL of the public portal where in SLAs of services offered on Public Cloud are furnished.
7	Operations	Cloud Service Provider should have an operational Public Cloud/private cloud/managed services, with a self- service portal, with at least 100 cloud customers or INR 100 crores annual billing from these services.	References of work orders/Purchase order/ Completion Certificate with name, address, contact person, and contact No, email address Or Self-Declaration may be provided (***Refer Form-3, Annexure F)***
8	Blacklist	Neither the current organization nor the holding company should have been debarred and/or blacklisted by any organizations of Govt. of India/ Central PSU/ State Govt entities as on the bid submission date.	CSP Self-Declaration from the authorized signatory ***(Refer Form-4, Annexure F)***
9	List of Services	CSP should have all the services listed in **Annexure-G** of the RFP document in ready-to-offer condition when bidding. CSP should also have the following cloud services in ready-to-offer condition under broad categories: 1. Core Infrastructure 2. Network Services 3. Security Services 4. Enterprise Management Support Services 5. Application Development Services 6. Data Analytics and AI/ML services 7. Productivity apps, such as email, collaboration, and calendaring 8. SaaS-based COTS Business applications for small/medium enterprises and organizations	CSP Self-Declaration on its letter head mentioning the publicly available weblink for Proof of service from CSP's online portal.

#	Category	Criteria	Documents Required
10	MeitY Empanelment	The CSP partnering with the MSP should be MeitY empanelled.	Self-declaration from the Authorized signatory of the CSP on their letterhead along with the URL of the public portal of MeitY, where in details of empanelment containing CSP name is visible.

Note:

I. Any bid failing to meet required above qualification criteria mentioned above, shall be disqualified.
II. MSP cannot submit more than one bid.
III. CSP can be part of more than one bid with different MSPs.
IV. Consortium bid is not allowed.
V. Any single company participating as both MSP & CSP will have to independently fulfil all the prequalification criteria of their respective roles as mentioned in **section 2.21** of this document.
VI. All certificates requested in the RFP (Pre-qualification/Technical qualification) should be valid as on the date of bid submission.

2.21.3. Technical Qualification Criterion

The evaluation of the technical bid will be carried out for MSP as well as CSP in the following manner:

a. The Technical bids of the pre-qualified bidders only, shall be opened for evaluation.
b. STPI will review the technical bids from shortlisted bidders to determine whether the technical bids are substantially responsive. STPI reserves the right to disqualify bids that are not substantially responsive.
c. The technical solutions proposed by the bidder in the bid documents will be evaluated according to the requirements specified in the RFP and the technical evaluation framework mentioned in the RFP.
d. STPI will set up a Tender Evaluation Committee (TEC) to evaluate the responses of bidders. The TEC will evaluate the response to the RFP and all supporting documents/documentary evidence.
e. Failure of bidders to submit the required supporting documents/documents may result in the rejection of their bids. All the eligible bidders will be required to make the presentations to TEC to supplement their bids.
f. TEC will assess the bidder’s response (i.e., proposal document, presentation etc.) and TEC will give score to the bidder based on the compliance and this score will be final.
g. The TEC may seek clarifications/additional documents from the bidders. The primary role of clarifications in the bid evaluation process is to clarify ambiguities and uncertainties that arise in bid evaluation documents.

h. If a bidder fails to submit the required clarifications within stipulated time to STPI, the TEC will evaluate the bid based on the technical bid already submitted and any documents submitted after the stipulated deadline shall not be taken for technical evaluation purpose.

i. To be eligible for the financial bid opening, the bidder must:

   i. Obtain a minimum overall technical score of 70 (seventy). Bidder must mandatorily demonstrate all the features as mentioned in the Demo/PoC section of RFP

For evaluation, the decision of the Tender Evaluation Committee shall be final. There will be no correspondence with the committee outside of the evaluation process. The Tender Evaluation Committee may request meetings or presentations with bidders for clarification or confirmation on their bids.

#	Technical Evaluation Parameters	Sub Marks	Marks
A	**Proposal document (A1+A2+A3)**		**25**
A1	**Approach and Methodology**		**5**
1	Understanding of project and potential market view	1	
2	Approach and Methodology for Customisation, Workflows, and self-service portal	1	
3	Service delivery approach	1	
4	Project management & Quality Assurance Plan	1	
5	Risks and Mitigation Plan	1	
A2	**Business Model**		**10**
1	Effective Utilization Plan for providing GCC, Hybrid Cloud & Edge services from: a. STPI's Data Centres – 1.5 Marks b. STPI's Edge locations – 1.5 Marks c. The investment assurance of the edge locations. (no. of edge location data centres to be utilized in 9 months from the date of award of contract) (1 mark for selecting minimum 10 Locations 2 marks for selecting minimum 15 Locations)	5	
2	Projected Revenue streams and Target market segments	1	
3	Funding and mobilization plan for the project	1	
4	Business plan including Go-To-market, Sales & marketing Plan, Salesforce deployment	3	
A3	**Proposed Technical Solution**		**10**
1	Proposed Technical solution including offered technologies, tools, Architecture of the complete platform of Hybrid & GCC, Multi-cloud/Hybrid cloud layer with implementation plan	3	
2	Proposed managed services plan including construct of roles & responsibilities	2	

#	Technical Evaluation Parameters	Sub Marks	Marks
3	Features and capabilities of key cloud security measurement components a. Identity and Access Management (IAM) – 1 Mark b. Intrusion Detection and Prevention - 1 Mark c. Vulnerability Management - 1 Mark d. DDoS Protection - 1 Mark e. Incident Response and Disaster Recovery - 1 Mark	5	
B	**Bidders experience in setting up, operating, and managing cloud operations**		**35**
1	The bidder must have successfully received the work order and have successfully executed/completed the project of establishing/deploying hybrid cloud and private clouds for any Central/State Government PSUs/ Government Departments/Nationalized Bank/Scheduled commercial bank/Large Private sector firms in India, during the last three financial year (2019-20, 2020-21, 2021-22) ending 31/03/2022. a. One project of value >=50 Cr.: 5 Marks or b. Two projects of value >= 50 Cr or One number of project of value >= 75 Cr: 10 Marks or c. Three projects of value >= 50 Cr orOne numberof project of value >= 100 Cr: 15 Marks The individual work order value for providing above mentioned Service shall be equal to INR 50 Crores ***Note:*** *Value of Completed work order will be considered as inclusive of all taxes.*	15	
2	Bidder/CSPs experience in providing system integration for hybrid cloud, Self-service portal, and tight coupling with cloud provisioning layer: a) For each such project - 2 Mark Maximum 10 marks can be awarded	10	
3	Bidders/CSP experience in application migration for Cloud services a) For each project of application/System migration from on-prem Infra to public/Hybrid cloud - 2 Mark per migration Maximum 10 marks can be awarded	10	

#	Technical Evaluation Parameters	Sub Marks	Marks
	Note: *Copies of relevant work orders or Client Certificate / contract documentation depicting the said experience credentials must be submitted for Section B-1,2 & 3;*		
C	**Technical Presentation and Demonstration**		**40**
1	Technical Presentation covering but not limited to the following pointers: i. Understanding of the project – 1 mark ii. Understanding of Proposed Business Model for the project – 1 mark iii. Demonstration of Utilisation Plan for STPI's Colocation Infrastructure for providing edge data centre/cloud services - 1 mark iv. Demonstration of Service delivery/operating model and Plan for innovative/additional services in future – 1 mark v. Approach for running overall operations including NOC, SOC & helpdesk – 1 mark	**5**	
2	Response to Q & A session with Evaluation Committee	**5**	
3	Demonstration of Managed services and capabilities as per the demonstration plan as referred in Annexure-I	**30**	

2.22. Bid Evaluation Process

Attempts by Bidders to influence STPI's bid evaluation, bid comparison, or contract award decisions may result in the rejection of the Bidder's bid and Bid Security/ EMD will be forfeited. During the bid evaluation process after bid opening, bidders are not permitted to make inquiries until the final decision has been disclosed to the winning bidder.

The Committee /its authorized representatives and the STPI office may make any inquiries/request for clarifications from bidders, bidders must provide the same within the given time frame else bids from such non- responsive bidders will be rejected.

STPI reserves the right to accept any bid, and to cancel/abort the tender procedure and reject all bids at any time prior to award of contract, without thereby incurring any legal responsibility to the affected bidder or bidders, of any duty to inform the affected bidder of the grounds for STPI's motion and without assigning any reasons.

Printed terms and conditions of the MSPs will not be considered as forming part of their bid. In case any terms and conditions of the tender document are not acceptable to the bidder, the bid shall be summarily rejected.

2.22.1. Technical Bid Evaluation

Prior to the detailed evaluation of the Technical Bids, STPI shall determine whether each bid is (a) complete, (b) is accompanied by the required information and documents and (c) is substantially responsive to the requirements set forth in the RFP documents.

The STPI will form a Tender Evaluation Committee (TEC), which will evaluate all i.e., prequalification, technical & commercial bids received in response to this RFP. The findings of the said Committee and subsequent decision of the STPI shall be final and binding on all the bidders. Only those bidders, who will fulfil all the criteria / requirements mentioned in the bid, shall be eligible and qualified for technical scrutiny as per the evaluation framework given in the **section 2** of this RFP.

Bidders should clear all technical evaluation parameters, to qualify for opening of the Commercial Bid.

STPI decision in this regard will be final and binding on the bidders. STPI may at its sole discretion, waive any informality or non-conformity or irregularity in a Bid Document, which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

The bidder who will score 70 Marks or more in the Technical Qualification criteria will be eligible to participate in the commercial evaluation. The bidder who has scored less than 70 marks will get disqualified and will not be able to participate further.

The weightage of the total technical marks scored by the bidder will be 70%.

2.22.2. Commercial Bid Evaluation

i. After the successful completion of the technical bid evaluation process, the technically qualified bidders will be notified to participate in Commercial Bid opening process and will be opened on the notified date and time.

ii. The Commercial bid will then be evaluated, and the non-compliant bids are liable to be disqualified at STPI discretion.

iii. The **weightage of the total commercial marks scored by the bidder will be 30%**.

iv. The normalised commercial score of the bidder will be calculated as per the given table below.

Slabs	**Revenue earned (in Cr)**	**Weightage (%)**	**Revenue % Share to STPI (R)**	**Marks (out of 100)**	**Weighted Marks**
Slab 1	0-100	60	A	M1	W1 = (0.60*M1)
Slab 2	101-500	30	B	M2	W2 = (0.30*M2)
Slab 3	>500	10	C	M3	W3 = (0.10*M3)
Normalised Commercial Score(T)					**W1+W2+W3**

v. The variables A, B, C are the revenue share that bidder must quote w.r.t revenue slabs given in the table above. Hence, Variable A corresponds to slab 1, B to Slab 2, C to Slab 3

vi. The bidder cannot quote the revenue share less than or equal to the previous slab therefore revenue share will be greater than the preceding value. i.e., B>A, C>B,

vii. The bidder must quote revenue share in percentage and in whole number.

viii. M1, M2 and M3 are the scoring marks that bidder will get per slab.

ix. The calculation of the marks will be comparative w.r.t to the quotation received from the other bidders

x. The bidder who will quote the highest % revenue share (R) for the respective slab and will get highest score of 100, here called as **S1**

xi. The score of the other bidder **S2** for the same slab (e.g., Slab 1) will be calculated as per the formula given below if **S1** has received highest marks for that particular slab or vice- versa.

S2 = 100 – {(100/A of S1) * (A of S1- A of S2)}

xii. The scoring will be done by the similar method for all the three slabs respectively.

xiii. The W1, W2 and W3 are the normalised score per slabs 1,2 and 3. They are calculated by multiplying marks scored by bidder (M1, M2 and M3) with the respective weightage i.e. (60%,30% and 10%)

xiv. Bidder deviating from the above clauses will be disqualified from the commercial bid

xv. The Total value i.e., T will be the normalised commercial score, it will be calculated for each bidder

xvi. The calculation of the revenue sharing will be on the linear basis or non-graded basis

For example, If the revenue earned is 130 Cr. then the revenue share% of slab 2 on will be applicable on whole revenue earned i.e. 130 Cr.

xvii. Bidder achieving the **highest Normalised Commercial Score** will get selected and called as **C1.**

2.22.2.1. Illustration: Evaluation of Commercial Score

Revenue Slabs	**Slab-wise Weight**	**Revenue Share**			**Normalised Scores**			**Weighted Scores**		
		B1	**B2**	**B3**	**B1**	**B2**	**B3**	**B1**	**B2**	**B3**
0-100	**60%**	15	12	10	100.00	80.00	66.67	60.00	48.00	40.00
101-500	**30%**	16	18	26	61.54	69.23	100.00	18.46	20.77	30.00
>500	**10%**	17	18	30	56.67	60.00	100.00	5.67	6.00	10.00
Final Scores								**84.13**	**74.77**	**80.00**

Out of the given three slabs:

a) 0-100 – bidder B1 has given the highest revenue share of 15% therefore 100 marks has been awarded and B2 and B3 has been awarded marks comparatively. If we compare it with the commercial evaluation criteria, then B1 has become the S1 (100 marks) and B2 as S2 (comparative scoring).

b) 100 – 500 - bidder B3 has given the highest revenue share of 26% therefore 100 marks has been awarded and B1 and B2 has been awarded marks comparatively similarly If we compare it with the commercial evaluation criteria, then B3 has become the S1 (100 marks) and B2 as S2 (comparative scoring).

c) >500 bidder B3 has given the highest revenue share of 30% therefore 100 marks has been awarded and B1 and B2 has been awarded marks comparatively. similarly, if we compare it with the commercial evaluation criteria, then B3 has become the S1 (100 marks) and B2 as S2 (comparative scoring).

d) The scores were normalised by multiplying the respective weightage against each slab as shown in the table above. Hence W1 for B1 is 60, W2 for B1 is 18.4 and W3 for B1 is 1.70.

e) The scores were added together to achieve the final Total Normalised Score, T for B1 is 80.16.

f) The bidder B1 has achieved the highest score i.e., 80.16. therefore, bidder B1 will be selected and called as C1

<u>Bidders to note that the table mentioned above is just for illustration purpose, only to showcase the commercial bid evaluation.</u>

2.23. Award Of Contract

2.23.1. Notification of Award (NoA)

STPI will determine Final Score (FS) based on scores obtained by Bidders in Packet 1 and 2 and will announce the highest scorer bidder (H1) for Notification of Award (NoA).

2.23.2. Final Score Calculation (QCBS)

The final score will be calculated through Combined Quality Based System (QCBS) method based with the following weightage:

a) Technical: 70%
b) Commercial: 30%

Final Score (FS) = (0.70 x Normalized Technical score) + (0.30 x Normalized Commercial Score)

I. The Bid of the Bidder, who obtains the highest final score value, will be rated as the best bid and the contract will be awarded to that Bidder. The bidder will be called as H1

II. If successful bidder as decided on basis of commercial l score, fails to sign agreement or perform its obligation mentioned in the RFP then its bid will be rejected and execution of bid security declaration/ EMD will be forfeited. STPI may invite the bidder with next highest final score for consideration as successful bidder.

III. The successful bidder shall be notified on its selection in writing or by email. The successful bidder shall also be issued a Letter of Intent confirming its selection.

IV. If two or more bidders have the same final score than the bidder having the higher technical score will be selected. If the technical score as well as commercial score are found to be same which is the rarest possibility, then the bidder who has quoted the higher share of revenue in the first slab will get selected.

V. Highest rank (H1) bidder will be given first preference to come onboard as partner MSP with STPI for setting up GCC and hybrid cloud.

Section III: General Terms and Conditions

3.1. Confidentiality of RFP

All materials/information shared with the bidder during this procurement process, as well as the subsequent resulting project after this process with the successful bidder will be treated as confidential and should not be disclosed to any unauthorized person/agency under any circumstances.

The Bidder shall bear all costs associated with the preparation and submission of its bid and STPI shall in no event be liable for such costs, regardless of the course or outcome of the bidding process.

The successful bidder is required to maintain the highest level of secrecy, confidentiality, and privacy regarding the project. Additionally, the successful bidder shall keep confidential all the details and information about the project, including systems, facilities, operations, management, and maintenance of the systems/facilities. STPI retains the right to prevent, stop and if required take the necessary punitive action against the successful bidder for any unauthorized disclosure. The successful bidder should provide non-disclosure agreement in the format provided by STPI.

a. For clarification, the aforementioned provisions do not apply to the following information: information already available in the public domain.
b. information which has been developed independently by the successful bidder.
c. information which has been received from a third party who had the right to disclose the aforesaid information.
d. Information which has been disclosed to the public pursuant to a court order.

3.2. Arbitration

a) In case any dispute or difference arises out of or in connection with or the carrying out of works (whether during the progress of the works or after their completion & whether before or after the termination, abandonments, or breach of contact) except as any of the accepted matters, provided hereunder, the parties hereto, shall first endeavour to settle such disputes of differences amicably.

b) If both the parties fail to reach such amicable settlement, then either party (The Purchaser or Contractor) may (within 20 days of such failure) give a written notice to the other party requiring that all matter in dispute or difference be arbitrated upon. Such written notice shall specify the matters which are in difference or differences of which such written notice has been given and no other shall be reoffered to the arbitration of a single arbitrator, to be appointed by both the parties or in case of disagreement as to the appointment of a single arbitrator, to that of two arbitrators, one to be appointed by each party or in case of said arbitrators not agreeing then, to the umpire to be appointed by the arbitrators in writing before entering upon the references. Provisions of Indian Arbitration & Conciliations Act, 1996 or any statutory modification or re-enactment thereof and rules framed there under from time to time shall apply to such arbitration.

c) The provisions of the Arbitration and Conciliation Act, 1996 shall be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules, or re-enactments thereof.

d） The venue of Arbitration shall be at Delhi.

3.3. Indemnification

The Managed Service Provider agrees to indemnify and hold harmless STPI and its officers, employees, and agents against all losses, claims, damages, liabilities, costs (including reasonable legal attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from

a) Any misstatement or any breach of any representation or warranty made by the MSP or

b) The failure by the Managed Service Provider to fulfil any covenant or condition contained in this Agreement, including without limitation the breach of any terms and conditions of this Agreement by any employee or agent of the MSP. Against all losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created Managed Service Provider pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by Managed Service Provider pursuant to this Agreement, or the SLAs,

(I) infringes a copyright, trademark, trade design enforceable in India,

(II) infringes a patent issued in India

or

(III) constitutes misappropriation or unlawful disclosure or use of another Party's trade secretes under the laws of India (collectively, "Infringement Claims"); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by

Implementation of Project by itself or through other persons other than Managed Service Providers or its sub-contractors.

or

Third Parties (i.e., other than MSP or sub-contractors) at the direction of STPI

c) Any compensation / claim or proceeding by any third party against STPI arising out of any act, deed, or omission by the Managed Service Provider or

d) Claim filed by a workman or employee engaged by the Managed Service Provider for carrying out work related to this Agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts enough to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

e) Jurisdiction: In case of any litigations between the parties to this agreement, the Courts at Delhi shall have the jurisdiction.

3.4. Severability & Waiver

a) If any provision of the resultant Agreement or the SLAs, 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 the resultant Agreement or the SLAs or the remainder of the provisions in question which shall remain in full force & effect. The relevant Parties shall negotiate in good faith to agree to substitute for any illegal, invalid, or unenforceable provision a valid & enforceable provision which achieves to the greatest extent possible the economic, legal & commercial objectives of the illegal, invalid, or unenforceable provision or part provision within seven (7) working days.

b) No failure to exercise or enforce & no delay in exercising or enforcing on the part of either Party to the resultant Agreement or the SLAs of any right, remedy or provision of the Agreement or the SLAs 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 any other right or provision.

3.5. Subsequent Legislation

If on the day of submission of bids for the contract, there occur changes to any National or State stature, Ordinance, decree or other law or any regulation or By-laws or any local or other duly constituted authority or the introduction of any such National or State Statute, Ordinance, decree or by which causes additional or reduced cost to the MSP, such additional or reduced cost shall, after due consultation with the MSP, be determined by the concerned authority of STPI and shall be added to or deducted from the Contract Price with prior approval of competent authority and STPI shall notify the MSP accordingly.

STPI reserve the right to take decision in respect of addition/reduction of cost in contract.

3.6. Modification and Withdrawal of Bid

a) Modification of the submitted bid shall be allowed online only till the last date and time of submission of the bid and the bidder may modify and resubmit their bid online as many times as it may wish within this period. This resubmission can be done, using ‘Rebid’ option of the portal.

b) Bidders may withdraw their bids online using ‘Withdrawal’ option of the portal, within the last date of bid submission. However, upon such withdrawal, the bidder shall not be allowed to resubmit its bid pursuant to this Notice Inviting Tender (NIT). As such, bidder is advised not to use this option, unless the bidder is certain not to participate in this tendering process again.

c) No withdrawal/ modification is allowed after the end date and time of bid submission

3.7. Bidders or their owners from country sharing land border with India

In Compliance to insertion of Rule 144 (xi) in the General Financial Rules (GFRs), 2017 vide office OM no. 6/18/2019-PPD dated 23" July 2020 issued by DOE, Ministry of Finance, Government of India, the following is mandatory:

Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority DPIIT, New Delhi.

Bidder (including the term tenderer, consultant, or service provider in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated here in before, including any agency branch or office controlled by such person, participating in a procurement process.

Bidder from a country which shares a land border with India for the purpose means:

I. An entity incorporated, established, or registered in such a country; or
II. A subsidiary of an entity incorporated, established, or registered in such a country; or
III. An entity substantially controlled through entities incorporated, established, or registered in such a country; or
IV. An entity whose beneficial owner is situated in such a country; or
V. An Indian (or other) agent of such an entity; or
VI. A natural person who is a citizen of such a country; or
VII. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

or

A System Integrator/Turnkey Award which is offering products/services from entities falling under any of the above.

The beneficial owner for the purpose of **point iv** above will be as under:

a) In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means. Explanation:

I. Controlling ownership interest means ownership of or entitlement to more than twenty-five per cent. of shares or capital or profits of the company.
II. Control shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b) In case of a partnership firm, the beneficial owner is the natural person(s)who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership.

c) In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals.

d) Where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

e) In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

An Agent is a person employed to do any act for another, or to represent another in dealings with third person. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority. Bidders will submit the certificate for Compliance along with their Bid/offer. Bidders may please note that in the event of acceptance of their bid on the certificate for compliance given by them and if the same is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law.

3.8. Obligation to maintain insurance

In connection with the provision of the Services, the Successful bidder must have and maintain for the Agreement Period, valid and enforceable insurance coverage for:

a) Public liability; either professional indemnity or errors and omissions
b) Workers' compensation as required by law
c) For all the Data Centre infrastructure & equipment provided by bidder
d) Fire Insurance
e) Third Party liability

The successful bidder shall cover insurance for all the infrastructure & equipment for one year beyond contract period/termination of contract

3.9. Survivability

The termination or expiry of the resultant Agreement or the SLAs for any reason shall not affect or prejudice any terms of the Agreement, or the rights of the Parties under them which are either expressly or by implication intended to come into effect or continue in effect after such expiry or termination.

3.10. Force Majeure

a. Definition:

i. For the purposes of this Agreement, “Force Majeure” means an event which is beyond the reasonable control of a Party, and which makes a Party’s performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by government agencies.

ii. Force Majeure shall not include (1) any event which is caused by the negligence or intentional action of a Party or such Party’s Sub-contractor or agents or employees, nor (2) any event which a diligent Party could reasonably have been expected to both (a) consider at the time of the conclusion of this Agreement, and (b) avoid or overcome in the carrying out of its obligations hereunder.

iii. Force Majeure shall not include insufficiency of funds or failure to make any payment required hereunder.

b. No breach of Agreement

i. The failure of a MSP to fulfil any of its obligations hereunder shall not be a breach of, or default under, this Agreement in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all reasonable precautions, due care, and reasonable alternative measures, all with the objective of carrying out the terms and conditions of this Agreement.

c. Measures to be taken

i. If an MSP affected by an event of Force Majeure shall notify STPI of such event as soon as possible, and in any event not later than 14 (fourteen) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give notice of the restoration of normal conditions as soon as possible.

ii. The MSP shall take all reasonable measures to minimize the consequences of any event of Force Majeure.

d. Extension of time

i. Any period within which a Party shall, pursuant to this agreement, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action because of Force Majeure

3.11. Obligations of STPI

Without prejudice to any other undertakings or obligations of STPI under the Agreement, the STPI shall perform the following:

1. To support successful bidder in marketing activities (e.g., support in targeting the Govt. clients) and GTM strategy.
2. STPI will help in business development and strategizing by the MSP, and both MSP & STPI shall work together for achieving business success however MSP needs to own the overall responsibility
3. Handing over of the earmarked space, contiguous racks with required power and cooling to the Successful Bidder for setting up GCC and Hybrid Cloud.
4. Access of MSP and CSP manpower resources to STPI Data Centres with defined process

3.12. Special Terms & Conditions

This e-Tender Notice shall be deemed to be part of the Contract Agreement to be entered into between STPI and the successful bidder.

a) Purchaser reserves the right to postpone the date of receipt and opening of bid or to cancel the tender without assigning any reason whatsoever, and STPI shall bear no liability, whatsoever, consequent upon such a decision. STPI reserves the right to reject any or all the bids without assigning any reasons whatsoever at its sole discretion. Any such action shall not be called into question and the bidders shall have no claim or cause of action in that regard against STPI or its officers, employees, consultants, agents, successors, or assignees for rejection of its bids. Neither STPI nor its employees or advisers shall entertain any claim of any nature, whatsoever, including without limitation, any claim seeking costs, expenses, or damages in relation to the preparation or submission of bids.

b) Notwithstanding anything stated above, STPI reserves the right to assess the bidder's capability and capacity to perform the scope of work envisaged hereunder satisfactorily, should the circumstances warrant such assessment in the overall interest of STPI.

c) No conditional bid shall be accepted.

d) STPI makes no representation or warranty, express or implied, as to the accuracy, correctness and completeness of the information contained in the Bid Documents. Each bidder must conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information and obtain independent professional advice on the legal, financial, regulatory and taxation consequences of entering into any agreement or arrangement in relation to the same from appropriate sources to satisfy itself that the Bid Documents are complete in all respects.

e) While the Bid Documents have been prepared in good faith, neither STPI nor its consultants, officers or employees make any representation or warranty or shall have any responsibility or liability whatsoever in respect of any statements or omissions here from. Nothing in the Bid Documents shall be construed as legal, financial or tax advice. Any liability is accordingly expressly disclaimed by STPI, its consultants, partners, affiliates, their respective officers, agents, and employees even if any loss or damage is caused by any act or omission on the part of STPI, its consultants, partners, affiliates, their respective officers, agents, or employees, whether negligent or otherwise.

f) The selected MSP shall provide an online published catalogue for each service offered. The catalogue shall include detailed information about the service, including its features, benefits, pricing, and any relevant terms and conditions. The catalogue prices shall be comparable to the market rate. Published catalogue should be available on the self-service portal as well with choosing and purchasing the required services by the customers.

g) STPI will form a steering committee, which will have members from the selected MSP and STPI officials to finalize the rate card of the services offered as per the prevailing market rates. The rate card shall be reviewed on a “Yearly” basis, however in case of addition of new service, the inclusion and deliberation of the rate can be done at any point of time. Steering committee may also define the joint marketing plan including Go to Market (GTM).

h) In case, if STPI utilizing MSP's Cloud services or infrastructure for its in-house use, the MSP shall offer those at a minimum/discounted price. The discount %age will be decided mutually.

i) If the onboarded MSP is found to be incompetent to perform any task or the work done by the MSP is deemed unsatisfactory, STPI reserves the right to terminate the contract and award the work to any other competent bidder. In this regard, the decision of STPI will be final and binding, and the terminated agency shall have no claim against STPI for any loss or damages arising from such termination. Further, in this case, **section 3.15** (Termination Clause) and **section 3.16** (Exit Management Clause) of the RFP shall be applicable. This clause will survive the termination of this contract/agreement and will not affect any other rights or remedies available to either party under this termination contract/agreement or any applicable law.

j) MSP will adhere to the rate card as mutually decided with STPI. The services to the end customers will be provided as per the same rate card and in case of addition of any new services in future, MSP shall ensure that the services are provided to STPI based on the mutually agreed rates. Any deviation from the same shall be done with the prior written approval of STPI.

MSP shall ensure that the cloud services price (after discounts) offered to STPI shall be less than the offered price (for similar services) to any other organization for similar scale. If at any stage during the contract period MSP violates this clause, PBG may be forfeited and STPI reserves the right to terminate the contract without any liability to MSP.

3.13. Minimum business commitment

i. In the first year of operation (starting from the date of contract signing) MSP shall pay the minimum committed revenue share of 16 Lakhs (INR) or the actual revenue share (as per section 2.22.2) , whichever is higher, .

ii. In the second and third year of operation, MSP shall pay the minimum committed revenue share of 64 Lakhs (INR) each year or the actual revenue share (as per section 2.22.2), whichever is higher.

iii. Beyond third year of operation, the minimum committed revenue share will increase by 10 % year on year of the previous year's minimum committed revenue. However, MSP shall pay the actual revenue share (as per section 2.22.2) or the minimum committed revenue of corresponding year wherever is higher. e.g., If the minimum committed share in year n (where n>=3) is X, the minimum committed share in year n+1 will be 1.1*X.

iv. STPI will review the circumstances if MSP is unable to generate the minimum business. STPI shall have right to change/waive-off the minimum committed revenue.

v. In case the MSP fails to fulfil the above clause, then STPI reserves the right to terminate the contract with immediate effect, without any liability to the bidder and recovering any applicable penalty from the performance bank guarantee.

vi. If the business done by the MSP is not meeting the minimum committed revenue for 2 consecutive years, then as decided by Core Committee may onboard the (second highest) H2 or (third highest) H3 bidder on the same revenue share model.

vii. In case of extensive demand, the MSP may do further investment to provide services from the additional data centre location adhering to uniform SLA's and conditions of this RFP.

viii. The performance of the onboarded partner MSP shall be reviewed by Core Committee at the end of financial year.

ix. The revenue shared between STPI and the onboarded MSP shall be applicable on the revenue generated by the MSP from providing cloud services at STPI Data centres, excluding taxes.

x. In case of termination of the contract with the MSP, Termination clause 3.15 shall be applicable and the ownership of the assets (IT and Non-IT) shall remain with the STPI. In this scenario, the Exit Management clause will be applicable as per section 3.16.

xi. MSP shall install brand new infrastructure (IT components etc.) at STPI locations.

3.14. Payment Terms

1. The bill to the customers will be generated in the name of STPI.
2. Customers will deposit the amount against the bill generated by STPI directorate (decentralised billing).
3. Payment to the MSP shall be done quarterly in arrear, based on the ratio of the division of the revenue as quoted by the MSP in its commercial bid **Annexure-J**.
4. Format for the invoices will be shared with MSP after its successful onboarding.
5. STPI may ask the MSP the service utilisation/consumption report the format of the same will be decided after the onboarding of the MSP.
6. Before making payment to the MSP, each payment will undergo scrutiny for breach of SLAs and other factors and payment will be released to MSP after deducting the penalty amount (if any)
7. MSP will submit one copy of customer bills physically and through email to the STPI's.
8. Format for the invoices will be shared with MSP after successful boarding. Invoices shall be genuine and accurate in all respects.
9. The invoices raised by MSP to STPI should be inclusive of all taxes, duties, levies, and services.
10. After receiving of the detailed invoice, each invoice payment will undergo scrutiny for breach of SLAs and other factors and payment will be released to MSP after deducting the penalty amount (if any).
11. All payments agreed to be made by STPI to the MSP in accordance with scope, payment terms, SLAs and other terms and conditions mentioned in this RFP and Contract.
12. The mode of Payment will be ECS/NEFT/RTGS only.
13. The Process for revision of rates shall also be undertaken when there is a fluctuation (10% up or down) in the foreign exchange rate (USD).
14. All the payment shall be made in Indian Rupees (INR) currency only.
15. MSP shall deploy an automatic tool for SLA calculation on real time basis including billing and accounting tool for end customers with no need for any manual intervention. This tool shall be implemented during the Go Live Phase and need to be approved by STPI before final Go Live.
16. STPI will withheld additional 10% amount on division of the revenue share quoted by the MSP on quarterly/monthly payment cycle and same will be released after a year by after SLA penalty deduction, if any.
17. The penalty cap will be the 20% of the actual revenue or estimated revenue (whichever is higher) by the MSP for that particular year.

3.15. Termination

STPI may, terminate this Contract in whole or in part and forfeit the PBG, by giving the Successful Bidder a prior written notice of Forty-Five (45) days indicating its intention to terminate the Contract under the following circumstances:

a. Where STPI is of the opinion that there have been such Event of Default on the part of the Successful Bidder which would make it proper and necessary to terminate this Contract and may include part of the Successful Bidder to respect any of its commitments about any part of its obligations under its bid, the RFP or under this Contract.

b. Where it comes to the notice of STPI that the Successful Bidder is in a position of actual conflict of interest with the interests of STPI, in relation to any of services arising out of services provided under the resultant contract or this RFP.

c. Where the Successful Bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any

bankruptcy proceedings against the Successful Bidder, any failure by the Successful Bidder to pay any of its dues to its creditors, the institution of any winding up proceedings against the Successful Bidder or the happening of any such events that are adverse to the commercial viability of the Successful Bidder. In the event of the happening of any events of the above nature, STPI shall reserve the right to take any steps as are necessary, to ensure the effective transition of the project to replacement bidder, and to ensure business continuity; or
As a result of Force Majeure, the Successful Bidder is unable to perform a material portion of the Services for a period of not less than hundred and twenty (120) days. The selected bidder commits a breach of any of the terms and conditions of the bid. The selected bidder goes into liquidation, voluntarily or otherwise.

d. If the selected bidder fails to complete the assignment as per the timelines prescribed in the tender and the extension if any allowed, it will be a breach of contract. STPI reserves its right to cancel the order in the event of delay and forfeit the PBG as liquidated damages for the delay.

e. After award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, STPI reserves the right to get the balance contract executed by another party of its choice by giving one-month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which STPI may have to incur in executing the balance contract. This clause is applicable, if for any reason, the contract is cancelled.

f. STPI reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract. In case if the onboarded MSP is found incompetent to perform any task / deliver business as per the requirements of this RFP.

3.15.1. Termination- Violation of Law/Agreement

a. In the event of any content found to be in violation of any law or direction of statutory authority or found to be in contravention of Intellectual Property Rights (IPR) etc., STPI may suspend / terminate the Agreement with seven days' notice. STPI reserves the right to terminate the Agreement for any breach or non-observance or non-fulfilment of Agreement conditions that may come to its notice through complaints or as a result of the regular monitoring by giving forty-five (45) days of written notice. Wherever considered appropriate STPI may conduct an inquiry either sue moto or upon a complaint to determine whether there has been any breach or non-observance of the terms and conditions of the agreement. The successful bidder shall extend all reasonable facilities and shall endeavour to remove the hindrance of every type upon such inquiry. Notwithstanding any other rights and remedies provided elsewhere in the agreement, upon termination of the agreement:
b. Neither Party shall represent the other Party in any of its dealings.
c. The expiration or termination of the Agreement for any reason whatsoever shall not affect any obligation of either Party having accrued under the Agreement prior to the expiration or termination of the Agreement and such expiration or termination shall be without prejudice to any liabilities of either Party to the other Party existing at the date of expiration or termination of the Agreement.

3.15.2. Consequences of Termination

a) In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], STPI shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the MSP shall be obliged to comply with and take all available steps to minimize loss resulting from the termination/breach, and further allow the next successor MSP to take over the obligations of the erstwhile MSP in relation to the execution/continued execution of the scope of the Contract.

b) Nothing herein shall restrict the right of STPI to invoke the successful bidder Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity, and pursue such other rights and/or remedies that may be available to STPI under law or otherwise.

c) The termination here of shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

3.15.3. Consequences of Event of Default and Insolvency

Where an Event of Default subsists or remains uncured, STPI may be entitled to have one or more of the following recourses:

a. Impose any such obligations and conditions and issue clarifications as may be necessary to inter alia ensure smooth continuation of Services and the project which the Successful Bidder shall be obliged to comply with. This may lead to re- determination of the consideration payable to STPI as mutually agreed by STPI and the Successful bidder.

b. STPI may, by a written notice of suspension to the Successful Bidder, suspend all payments if any under the Contract, provided that such notice of suspension:
   i. shall specify the nature of the failure; and
   ii. shall request the successful bidder to remedy such failure within a specified period from the date of receipt of such notice of suspension.

c. Terminate the Contract either in Part or Full:
   i. All assets will be transferred to STPI at Nil cost as may be required to offset any losses caused to STPI. Because of such default, the MSP shall compensate STPI for any such loss, damages, or other costs, incurred by STPI in this regard; Successful Bidder after termination, will exit along with its brand associated with STPI. Cobranding will cease to exist after exit.
   ii. Invoke the PBG furnished by the Successful Bidder.

3.16. Exit Management

The exit management period starts, in case of expiry of contract, at least 12 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the MSP. The exit management period ends on the date agreed upon by the STPI or 12 months after the beginning of the exit management period, whichever is earlier.

In case of termination, 12 months exit period will be applicable, otherwise as decided by STPI. Ownership of all the assets deployed by MSP (IT and Non-IT) for cloud services shall remain with the STPI only.

3.16.1. Exit Management Plan

The MSP will provide STPI with a recommended exit management plan within 90 days of signingof the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

The project is a very strategic and complex in nature. It is necessary to have a comprehensive exit management strategyin place. The MSP shall need to ensure the following:

a) The MSP will submit a structured & detailed exit management plan along with the technical proposal.

b) Exit Management Plan shall be presented by the MSP and approved by STPI.

c) The MSP needs to update the exit management on a half yearly basis or earlier in case of major changes during the entire contract duration. This plan needs to be discussed and approved by the STPI.

d) The MSP will also submit a technical plan for transfer of applications, data, backup media, documentation, and any other asset of STPI from the Data Centre and DR site in case STPI decides not to continue further with MSP. The MSP will facilitate all such transfer with the chosen service provider of STPI. STPI reserves the right to verify that no data is left on the infra provided by MSP and the same are deleted from MSP assets before transition.

e) At the end of the contract period or during the contract period, if any other agency is identified or selected for providing services related to the MSP’s scope of work, the MSP will ensure that a proper and satisfactory handoveris made to the other agency. MSP will support in all respects and decision of STPI will be final in this regard.

f) All risks during the transition stage will be properly documented by the MSP and mitigation measures shall be planned to ensure a smooth transition without any service disruption.

g) In all the cases, the exit management period will start 6 months before the expiration of the contract/exit. The MSP will provide support for at least 6 months before the end of the O&M period or termination of the contract, as applicable at no additional cost to the STPI. In case of termination, the exit management period will start from effective date of termination, or such other date as may be decided by the STPI but no later than 12 months from effective date of termination

h) Closing off all critical open issues as on date of exit; All other open issues as on date of exit shall be listed and provided to the STPI.

i) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

j) The MSP will provide necessary knowledge transfer and transition support. The deliverables are indicated below:

   i. Updated exit management plan on a periodic basis.

   ii. Complete documentation for the entire system handed over to the STPI/identified agency.

   iii. Handover of all AMC support related documents, credentials etc. for all OEM products supplied/maintained in the system. Handover MOUs signed for taking services taken from third partiessuch as digital signature agencies, etc.

   iv. Handover of the list of complete inventories of all assets created for the project.

   v. Assisting the new agency/the STPI with the complete audit of the system including licenses and physicalassets.

   vi. Detailed walk-throughs and demos for the solution. G. Hand-over of the user IDs, passwords, securitypolicies, scripts etc.

k) Knowledge transfer of the system to the incoming MSP to the satisfaction of the new MSP as per the given timelines

l) The MSP will be released from the project once successful transition is completed by meeting the parametersdefined for successful transition.

m) The MSP will ensure that the data, assets, images in the datacentre and DR site must be preserved for a period of12 months from the end of contract. This shall not be deleted/destroyed without the prior consent of the STPI

n) The commercial quoted by the bidder to include transition costs also and STPI will not pay any additional fees fortransition.

o) Plans for provision of contingent support to the project and Replacement MSP for a reasonable period(minimum one month) after transfer

p) The MSP shall provide the following details to STPI:

   I. All the customer KYC details who are availing the services, service details & its charges, billing cycle etc.

   II. Service Provider details from whom services availed.

   III. Equipment OEM details along with AMC & Warranty

q) During Exit, Successful bidder will indemnify losses completely, if any, to the customers and shall meet all the obligations towards Customers, Third Party Service providers, OEMs etc. before handing over the infrastructure and clients to STPI/appointed agency.

r) The assets shall be free from any financial obligations owing to any of the financial institutions/banks, clients, service providers etc.

s) Any hardware purchase made as part O&M of Non-IT infra will not be taken back by MSP during exit process.

t) MSP to ensure minimum of one year EoL(end of life) status for all Non-IT infra (only in case of edge location DC) at the time of exit.

u) All outstanding charges must be cleared including payments or any additional infrastructure to STPI, if not, theseshall be deducted from the Performance Bank Guarantee.

3.16.2. Confidential Information, Security and Data

MSP will promptly on the commencement of the exit management period, supply to STPI or its nominated agenciesthe following:

a) Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to Surveillance Project, Project's Intellectual Property Rights; any other data and confidential information related to the Project.

b) Project data as is required for purposes of the Project or for transitioning of the services to its Replacing Successful Bidder in a readily available format.

c) All other information (including but not limited to documents, records, and agreements) relating to the services to enable STPI and its nominated agencies, or its Replacing MSP to carry out due diligence to transition of the Services to STPI or its nominated agencies, or its replacing MSP (as the case may be).

3.16.3. Transfer of Projects Assets

a) Before the expiry of the Exit Management Period, all non-IT Project assets (only in case of edge location DC) and any of the infrastructure shall have been renewed and cured of all defects and deficiencies as necessary so that the Project is compliant with the specifications and standards set forth in the Agreement, RFP, and any other amendments made during the Contract Period

b) Before the expiry of the exit management period, the bidder will deliver relevant records and reports pertaining tothe Project and/or the STPI and its design, implementation, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the divestment date

c) The Bidder will provide the STPI with a complete and up to date list of the Assets to be transferred to the STPI/STPI's appointed agency within 30 days of start of Exit Management Period.

d) The outgoing Bidder will pass on to STPI and/or to the replacement agency (if engaged by the STPI), the subsisting rights in any leased properties/ licensed products on terms not less favourable to the Department/ replacement agency, than that enjoyed by the outgoing Bidder.

e) Even during the Exit Management period, the Bidder shall continue to perform all their obligations and responsibilities as stipulated under this RFP, and as may be proper and necessary to execute the scope of work in terms of the RFP and Bidder's Bid, in order to execute an effective transition and to maintain business continuity

f) All solutions provided by successful bidder under the scope of this RFP should be MSP agnostic to avoid any complication/interoperability issues during the asset transfer/hand over at time of exit/contract termination. No proprietary service is to used/implement by the MSP. Any customization/ tools/ effort required for smooth transfer of assets arising out of interoperability issue will be borne by the MSP.

g) All equipment and solutions utilized to deliver the project scope should have valid service contract and should not be under end of life/end of support during project duration.

h) The MSP will share the details of all existing service contracts and agreements executed with current MSPs, sub-contractor, CSP to STPI at yearly basis.

i) On premature termination of the contract, the ownership of assets (IT and Non-IT) shall remain with the STPI only.

3.16.4. Employees

Promptly on request at any time during the exit management period, the MSP will, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to STPI a list of all employees (with job titles and communication address) of the MSP, dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the MSP Successful Bidder, STPI or Replacing MSP may make an offer of contract for services to such employee of the MSP and the MSP will not enforce or impose any contractual provision that would prevent any such employee from being hired by STPI or any Replacing MSP

3.16.5. Rights of Access to Information

At any time during the exit management period, the MSP will be obliged to provide an access of information to STPI and / or any Replacing MSP in order to make an inventory of the Assets (including hardware / Software / Active/ passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other materialrelated to the Surveillance Project.

3.16.6. Payments during Exit Management Period

a. Payment to the outgoing Bidder will be made to the tune of last set of rendered Services / Deliverables (includingparts thereof) as stated in the terms of Payment Schedule, subject to SLA requirements. Without prejudice to any other rights, the STPI may retain such amounts from the payment due and payable by the STPI to the Bidder as maybe required to offset any losses, damages or costs incurred by the STPI as a result of the termination of Bidder or due to any act / omissions of the Bidder or default on the part of Bidder in performing any of its obligations with regard to this RFP.

b. Nothing herein the Exit Management Schedule shall restrict the right of the STPI to invoke the Bank Guarantee and other Guarantees furnished hereunder, enforce the Deed of Indemnity, and pursue such other rights and/or remedies that may be available to the STPI under law.

3.16.7. Transfer of Confidential Information and Data

a. The Bidder will on the commencement of and during the exit management period supply to the Department the following:
   i. Information relating to the current Services rendered and customer satisfaction surveys and performance data.
   ii. relating to the performance of Bidder's subcontractor in relation to the Services.
   iii. Documentation relating to the STPI's Intellectual Property Rights.
   iv. STPI/ Department's data and Confidential Information.
   v. All current and updated Project data as is reasonably required for purposes of Department or its nominated agencies transitioning the Services to its replacement Bidder or its nominated agencies in a readily available format nominated by Department.
   vi. All other information (including but not limited to documents, records, and Agreements) held or controlled by the Bidder which they have prepared or maintained in accordance with the RFP, the Project implementation, and the SLA relating to any material aspect of the Services or as is reasonably necessary to affect a seamless handover of the Project to the Department or its nominated agencies or its replacement Bidder.

b. Before the expiry of the exit management period, the Bidder shall deliver to the Department all new or updated materials from the categories set out above and shall not retain any copies thereof.

c. For the purposes of this Schedule, anything in the possession or control of Bidder or its associated entity is deemed to be in the possession or control of the Bidder. Before the expiry of the exit management period, unless otherwiseprovided under the Agreement, Department shall deliver to the Bidder all forms of Bidder Confidential Information, which is in the possession or control of the Department or its users.

3.16.8. Rights of Access to Premises

a. At any time during the Exit Management Period, where Assets are located at the Bidder's premises, the Bidder will 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) the STPI, and/or any appointed agency in order to make an inventory of the Assets.

b. The Bidder shall also give the STPI or its nominated agencies right of reasonable access to the Bidder's premises andshall procure the STPI or its nominated agencies and any replacement Bidder rights of access to relevant third-party premises during the exit management period and for such period following termination or expiry of the Agreement as is reasonably necessary to migrate the services to the STPI or its nominated agencies

3.17. Service level Agreement

a) The MSP needs to comply with service levels during the operations of the system. The MSP shall assume responsibility for measuring the Service Level Agreements (SLAs) at various levels, employing an enterprise monitoring tool on a periodic basis. SLA management tool needs to be deployed to manage the SLAs by MSP.

b) All SLAs and corresponding SLA reports need to be configured, monitored, calculated, and delivered/provided to the end user and STPI SPOC by the bidder. All SLA to be monitored using SLA monitoring tool to be brought in by the bidder. SLA monitoring tool should be capable of monitoring and reporting SLA of on-prem infrastructure and cloud services on all parameters including but not limited to the details furnish in this section. SLA should be configured at the beginning of the project and will be verified during UAT /Signoff

c) The liquidated damages specified in the SLAs of this RFP correspond to their respective severity levels. The table below illustrates the proposed framework for performance penalties in case of failure to meet the Service Level Targets

Sr. No.	Impact Level	Penalty as a percentage of Monthly payment applicable
1	9	10%
2	8	8%
3	7	4%
4	6	2%
5	5	1%
6	4	0.50%
7	3	0.40%
8	2	0.30%
9	1	0.20%

d) The MSP should have its own comprehensive monitoring solution. The MSP should use the same tool to do an integrated monitoring of the entire IT and Cyber security infrastructure at Data Centre, DR site, network, and office equipment. The monitoring tool should provide automated status issues at each layer of STPI infrastructure, network, and applications. MSP to propose suitable service desk tool for the project requirements and include in the proposal.

e) The MSP needs to carry out real-time monitoring as well as reporting of SLA parameters and will also be required to provide an integrated and automated monitoring report to STPI on monthly basis, or as requested by STPI. All SLAs to the extent possible should be monitored through the automated tools provided by MSP. The minimum service levels that need to be measured and adhered to, are detailed below. Bidders can propose to adhere to higher service levels than stated below and additional parameters to strengthen their technical proposal.

f) The Service Level Agreements have been logically segregated in the following categories:

i. Project Implementation
ii. Monitoring, Measuring and Reporting Service Levels
iii. System Availability
iv. Recovery Time Objective
v. Network Connectivity and Bandwidth
vi. Operations support for DC and DR sites
vii. Security operations and management
viii. Service Desk
ix. Service Provisioning
x. CSP

SLA treatment shall be based on the root cause analysis and accordingly the SLA treatment shall be given to the ticket for the issue

3.17.1. General SLA Requirements

i. The MSP shall ensure compliance to uptime and performance requirements of project as indicated in the below given SLA tables of RFP. Any upgrades/major changes to the setup shall be accordingly planned by the MSP to ensure the SLA requirements are adhered.

ii. All the SLAs must be managed by the MSP. Any gap between RFP SLA and SLA provided by respective OEM of the IT infrastructure and Cyber Security components shall be managed by the MSP with no impact on STPI.

iii. SLAs shall be applicable from date of go-live.

3.17.2. Project Implementation

In the event if MSP fails to meet the project implementation timelines, as agreed upon in the contract, STPI shall be entitled to impose a penalty as per listed below table:

Sr. No	Period	Applicable Penalty
1.	Delay up to 4 weeks	INR 2.5 lacs per week
2.	Delay from 4 to 8 weeks	INR 5 lacs per week
3.	Delay from 8 to 12 weeks	INR 10 lacs per week
4.	Delay beyond 12 weeks	PBG will be forfeited, and contract may be terminated on discretion of STPI

Note: MSP will have to pay the penalties within 3 months else the PBG will be forfeited. This is only applicable for missing the Project Implementation timelines

3.17.3. Monitoring, Measuring and Reporting Service Levels

a) MSP shall accurately monitor, measure and report on the performance of the Solution, the O&M Services, and the Services against all the Service Levels throughout the Term and as set out in Section IV– Scope of Work.

b) For the purpose of fulfilling its obligations, MSP shall:

i. Fully implement and comply with the Service Level and attainment of deliverables being set out in Section IV – Scope of Work.

ii. Provision, maintain and use adequate and auditable tools and procedures so as to be able to fully perform all its obligations under this Schedule, including a Service Level monitoring tool and Enterprise Management System (EMS) tool that automatically monitors Service Levels in real time and provides automated reports can be accessed by Customer in real time through a consolidated dashboard.

iii. Provides automated status issues at each layer of Customer infrastructure, network, and applications; and obtain and maintain access to the Customer ITSM Tool as necessary to monitor, measure and report on the performance of the Solution, the O&M Service and the Services.

iv. Record all data created as part of its monitoring or measurement activities or otherwise in connection with the performance of the Services,

v. Make all such data available for checking and audit by Customer back up and store all such data in the ITSM Tool such that any part of the data can be readily extracted for analysis, reporting, auditing, and presentation purposes, as required by Customer.

vi. Make such data accessible and understandable to Customer in real-time via a secure website accessible only by Customer and those individuals authorized Customer; and submit a monthly MIS report covering all key details of compliance with the Service Levels.

vii. Create other reports, trend analysis and such other information as Customer may reasonably request to verify MSP's performance and compliance again the Service Levels.

c) Within five (5) Business Days at the end of each month MSP shall provide Customer with a written (paper or electronic) monthly report detailing the actual levels of performance of the Solution, the O&M Services, and the Services against the Service Levels in such month, together with:

   i. Details of the monitoring which has been performed by MSP in accordance with Project scope along with a summary of the performance-related issues identified by such monitoring.

   ii. A summary (and each RCA) of all Service Failures that occurred during the relevant month.

   iii. which Service Failures remain unresolved, including an assessment as to how long they will remain unresolved.

   iv. A statement of the Service Credits payable in respect of Service Failures which occurred during the relevant month together with supporting calculations.

   v. A total of the number of Service Failures that have occurred and the amount of Service Credits that have been incurred by MSP over the past twelve (12) months.

   vi. Relevant particulars of any aspects of MSP's performance which fail to meet the requirements of the Agreement; and such other detail as Customer may reasonably require to be included in the monthly report from time to time.

d) MSP shall provide the performance report against the Service Levels monthly.

e) MSP shall, throughout the Term and as set out in the project scope section (Section IV – Scope of Work), evaluate all data generated as part of the process of monitoring its performance against the Service Levels.

f) MSP shall, present Customer with regular proposals (no less than quarterly) on ways in which MSP shall optimize the performance of the Solution and the Services with which each Service Level relates.

g) MSP shall ensure that suitably qualified MSP Personnel attend and participate in regular Service Level evaluation meetings with Customer at such times and places for such purposes as Customer requires.

h) Notwithstanding MSP's obligations in relation to RCA, Customer may perform, or may appoint an Other third-party agency to perform, RCA on any Service Failure.

i) MSP acknowledges and agrees that all data created, handled and/or collected by it in connection with the performance of its obligations under this Schedule is deemed be Customer's Confidential Information

3.17.4. System Availability SLAs

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
1	IT Infrastructure and Service Availability	Measures availability of overall IT infrastructure and Cloud Services & Availability of all IT infrastructure systems for at least 99.9% of time measured monthly for a 24x7x365 period	Minimum 99.9% up time measured on a monthly basis for overall IT Infrastructure	Nil	Measured monthly and considered for 24x7x365 operations. Approved downtime shall be excluded from the calculation
			>= 99.8% to <99.9% up Time measured monthly for overall IT Infrastructure	5	
			>= 99.7% to <99.8% up time measured monthly for overall IT Infrastructure	6	
			>= 99.6% to <99.7% up time measured on a monthly basis for overall IT Infrastructure	7	
			>= 99.5% to <99.6% up time measured monthly for overall IT Infrastructure	8	
			<99.50% up time measured monthly for overall IT Infrastructure	9	
2			Maximum 70% capacity utilization.	Nil	

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
	IT Infrastructure capacity utilizations.	Measures capacity of on-prem physical IT resources such as compute, storage, networking, security devises etc. Capacity utilization maximum 70% of time measured monthly for a 24x7x365 time period	>= 70% to <75% capacity utilization.	5	Capacity of each individual IT and Security component in the Data Centre as well in DR measured independently monthly and considered for 24x7x365 operations.
			>75% to <80% capacity utilization.	6	
			>=80% to <85% capacity utilization.	7	
			>=85% to <90% capacity utilization.	8	
			<95% capacity utilization.	9	
3	Component Level IT Infrastructure (physical and virtual) and Cyber Security Availability on a 24x7 basis	Measures up time as per IT infrastructure and per Cyber Security component/device/tool basis (including all databases except e-CTS) Uptime = {1 – [(IT Infrastructure and Cyber Security Component/Devices/Tools downtime)/ (Total Time – Maintenance Time)]} Total Time shall be measured by calculating total business hours during the month in respect of each	Minimum 99.671% up time measured monthly for each component/device/tool	Nil	Availability of each individual IT and security component in the Data Centre as well in DR measured independently monthly and considered for 24x7x365 operations. Approved downtime shall be excluded from the calculation
			<99.671% measured monthly for each component/device/tool	0.01% of the entire monthly billing (Total Cloud platform) per month for each 0.10% downtime per unit beyond 99.671%	

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
		IT infrastructure component.			
4	Backup Reports	Daily backup report provided by MSP for backup of all systems conducted on the previous day. Target: No delay SLA shall be calculated on monthly basis for each delayed report in the month cumulatively	No delay	Nil	Backup report shall be submitted on daily basis for all backups conducted on previous day. SLA shall be calculated on monthly basis. Delay in each backup report is treated individually
			Delay of more than 1 day	1	
5	Completion of Failed Backup Jobs	**Definition**: Backup jobs that have failed as part of the overall backup schedule (daily, weekly, monthly) shall be reported within 1 hour of failure and re-conducted and completed within 4 hours of reporting. **Target:** No delay on completion of failed backup jobs for every hour of delay of completion of the backup job (failed), penalty percentage corresponding to the severity level shall be accumulated.	No delay	Nil	Measurement shall be done for adherence to both reporting and reconduct and completion timelines on monthly basis for each backup job that had failed during the month
			For every hour of delay in completion of failed backup jobs	1	

3.17.5. SLA for Time recovery Objectives

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
1	Recovery Time Objective	**RTO 60 Minutes** RTO shall be measured through DRM tool during DR drill or actual failover If any of the services under the DR drill plan/BCP plan do not meet the target RTO then this SLA will be considered as breached.	100% of target RTO	Nil	RTO shall be calculated for each incident of service unavailability beyond 60 minutes
			>= 99.0% to <100% achievement of target RTO	5	
			>= 98.0% to <99.0% achievement of target RTO	6	
			>= 97.0% to <98.0% achievement of target RTO	7	
			<97% achievement of target RTO	8	
2	Recovery Point Objective	RPO 15 mins.	100% of target RPO	Nil	
			>= 99.0% to <100% achievement of target RPO	5	
			>= 98.0% to <99.0% achievement of target RPO	6	
			>= 97.0% to <98.0% achievement of target RPO	7	

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
			<97% achievement of target RPO	8	

3.17.6. SLAs for Network Connectivity and Bandwidth

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
1	Availability of Network devices at all locations	Measures availability of overall internet links at the locations Availability of internet links for at least 99.5% of time measured monthly for a 24x7x365 time period.	Minimum 99.5% up-time measured monthly	Nil	Availability and uptime of overall internet links at all the locations measured monthly and considered for 24x7x365 operations. Approved downtime shall be excluded from the calculation
			>= 99.4% to <99.5% up-time measured monthly	5	
			>= 99.3% to <99.4% up-time measured monthly	6	
			>= 99.2% to <99.3% up time measured monthly	7	
			>= 99.1% to <99.2% up time measured monthly	8	
			<99.1% up time measured monthly	9	
2	Latency for all links	Latency is the average round trip time taken by a packet within a network. Latency will be	<= 4ms	Nil	Latency of all links at Location 1 and Location 2 measured monthly and considered for
			>4ms to 10ms	5	

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
		determined for each internet and intranet link at the Data Centre, DR site, replication links and links at the STPI offices and accordingly SLAs will be applicable for each link	>10ms to 15ms	6	24x7x365 operations. Approved downtime shall be excluded from the calculation
			>15ms to 20ms	7	
			>20ms to 30ms	8	
			>30ms to 40ms	9	
3	Jitter for all links	Jitter is defined as the variation in the latency between two locations. Jitter will be determined for each internet and intranet link at the Data Centre, DR site, replication links and links at the STPI offices and accordingly SLAs will be applicable for each link.	<30ms	Nil	Jitter of all links at Location 1 and Location 2 measured monthly and considered for 24x7x365 operations. Approved downtime shall be excluded from the calculation
			>30ms to 60ms	5	
			>60ms to 90ms	6	
			>90ms to 120ms	7	
			>120ms to 150ms	8	
			>150ms to 180ms	9	
4	Packet Loss for all links	Packet Loss is defined as the percentage ratio of total number of packets lost to total number of packets transmitted. Packet loss will be determined for each internet and intranet link at the Data Centre, DR site, replication links and links at the STPI offices	<0.5%	Nil	Packet loss for all links at Location 1 and Mohali measured monthly and considered for 24x7x365 operations. Approved downtime shall be excluded from the calculation
			>0.5% to 1%	5	
			>1% to 2%	6	
			>2% to 3%	7	
			>3% to 4%	8	

#	SLA Parameter	Definition & Target	Service Level	Impact Level	Measurement Mechanism
		and accordingly SLAs will be applicable for each link.	>4% to 5%	9	

3.17.7. SLAs for Operations Support [DC/DR components]

#	SLA Parameter	Description	Target	Service Level	Impact Level	Measurement Mechanism
1	Time to Resolve – Severity 1	Time taken to resolve the reported problem	For Severity 1, 100% of the incidents should be resolved within 60 minutes of problem reporting	% Of incidents with more response time <100% & >=99%	5	SLA shall be measured monthly for each incident individually from the time of incident reporting on 24x7x365 operations.
				% Of incidents with more response time < 99% & >= 98%	6	
				% Of incidents with more response time <98%	7	
2	Time to resolve –	Time taken to resolve the reported problem	100% of Severity 2 within 4 hours of problem reporting, Severity 3	% Of incidents with more response time	1	SLA shall be measured monthly for each incident individually from

#	SLA Parameter	Description	Target	Service Level	Impact Level	Measurement Mechanism
	Severity 2, 3 and 4		within 12 hours of problem reporting, Severity 4 within 48 hours of problem reporting	<100% & >=97%		the time of incident reporting on 24x7x365 operations.
				% Of incidents with more response time < 97% & >= 94%	2	
				% Of incidents with more response time < 94%	3	
3	Percentage of re- opened incidents	For all incidents that are marked as Resolved by the Service Provider but are re- opened by the client. This is calculated for all incidents reported within the month	<= 3%	% Of reopened incidents <=4 & >3%	2	SLA shall be measured monthly for each reopened incident individually on 24x7x365 operations.
				% Of reopened incidents <=5% & >4%	3	
				% of reopened incidents >5%	4	

3.17.8. SLAs for Security Operations and Management

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
1	SOC Event Sources Covered	The scope includes all the active devices from STPI Data Centre, DR site and end-user devices that can integrate with SIEM for event collection. % Of event sources covered = (Number of event sources from which log data is captured at SIEM/Number of IT components deployed within STPI Data Centre, DR site and others) x 100 **Target:** Event sources covered shall be = 100% Measured 24x7 basis per month (calculated at end of month) Any new device/component added to the Data Centre/DR site shall be integrated with SIEM before go-live	100%	Nil	SLA shall be measured on no. of active event sources that are integrated with SIEM vis-à-vis the total no. of active event sources that can be integrated with SIEM. SLA shall be measured on monthly basis for 24x7x365 operations.
			>= 99% & < 100%	4	
2	SOC - % of valid escalations for SOC	The scope includes all the incidents which are classified as security incidents in the service desk tool. Definition: % Of valid escalations by SOC Calculation: Formula = [(∑valid escalations)/ (∑valid escalations +	>= 98% & < 99%	5	SLA shall be measured based on average number of valid incident escalations done by a SOC analyst vis-à-vis total

<table>
<tr><th>S. No</th><th>SLA Parameter</th><th>Definition & Target</th><th>Service Level</th><th>Impact Level/Penalty</th><th>Measurement Mechanism</th></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4">∑missed escalations + ∑delayed escalations] *100
The security incidents logged in the service desk tool will be considered for SLA calculation. These incidents are classified based on the priority (Severity 1 to 3). There are three level of analysts (L1, L2, and L3) and the tickets are escalated by respective analyst to the next level based on the requirements
An escalation/ticket will be treated as valid escalation if the escalation is done within the stipulated timeline based on ticket priority (Severity 1 to 3) tabulated below:
<table>
<tr><th>Severity</th><th>SOC L1</th><th>SOC L2</th><th>SOC L3</th><th>Total Restoration time</th></tr>
<tr><td><b>Severity 1</b></td><td>15 min</td><td>15 min</td><td>NA</td><td><=1 hr.</td></tr>
<tr><td><b>Severity 2</b></td><td>1.5 hrs.</td><td>1.5 hrs.</td><td>NA</td><td><=4 hrs.</td></tr>
<tr><td><b>Severity 3</b></td><td>5 hrs.</td><td>5 hrs.</td><td>NA</td><td><=12 hrs.</td></tr>
<tr><td><b>Severity 4</b></td><td>12 hrs.</td><td>12 hrs.</td><td>NA</td><td><=48 hrs.</td></tr>
</table>
<b>Note:</b>
1. L3 is the highest level of escalation and there will not be any further escalation after SOC L3 for security incidents.
2. The same resource shall not act as L1, L2 and L3 for a single ticket.</td><td>>= 97% & < 98%</td><td>6</td><td rowspan="4">escalations calculated monthly for 24x7x365 operations.</td></tr>
<tr><td><97%</td><td>7</td></tr>
<tr><td>>=90%</td><td>Nil</td></tr>
<tr><td><= 90%</td><td>4</td></tr>
</table>

<table>
<tr><th>S. No</th><th>SLA Parameter</th><th>Definition & Target</th><th>Service Level</th><th>Impact Level/Penalty</th><th>Measurement Mechanism</th></tr>
<tr><td></td><td></td><td>3. Calculation shall be done on SOC on monthly basis.
<b>Target:</b> Percentage of valid escalations shall be >= 90%</td><td></td><td></td><td></td></tr>
<tr><td rowspan="5">3</td><td rowspan="5">Event to Incident Conversions</td><td rowspan="5">Definition: Events generated in SOC shall be converted to Security Incidents based on the SOPs defined and agreed mutually with STPI as per the Severity defined below:
<table>
<tr><th>Severity Level</th><th>Event to Incident Conversion Time</th></tr>
<tr><td>Severity 1</td><td>15 minutes</td></tr>
<tr><td>Severity 2</td><td>1 hour</td></tr>
<tr><td>Severity 3</td><td>4 hours</td></tr>
</table>
Target: 100% conversion of events to security incidents as</td><td>100% Conversion</td><td>Nil</td><td rowspan="5">SLA shall be calculated on average of all events generated in SOC and converted to security incidents within the given timelines and calculated on a monthly basis for 24x7x365 operations</td></tr>
<tr><td>>= 99% & < 100%</td><td>4</td></tr>
<tr><td>>= 98% & < 99%</td><td>5</td></tr>
<tr><td>>= 97% & < 98%</td><td>6</td></tr>
<tr><td>< 97%</td><td>7</td></tr>
</table>

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
		per pre- defined SOP and as per timelines stated above calculated on a monthly basis.			
4	Fine-tuning of security solutions	**Definition:** Submission of monthly report on fine-tuning carried out on all security solutions as well as proposed fine-tuning to be carried out for the next month. Any fine-tuning activity approved/requested by STPI shall be implemented within 7 days from the date of approval. **Target**: No delay in both report submission as well as approved/requested fine-tuning activities. If anyone of the activities is delayed, then penalty corresponding to the respective delay and associated severity level will be applied.	No Delay	Nil	SLA shall be calculated for each instance of delay in report submission or completion of the approved finetuning activity for the given month
			Delay of 1-3 days	1	
			Delay of more than 3 days	2	
5	SOC Use Case Implementation	**Definition**: All new use cases approved/requested by STPI shall be implemented within one working of approval **Target:** No delay. If any use case implementation is delayed, then penalty corresponding to the respective delay and associated severity level will be applied.	No Delay	Nil	SLA shall be calculated for each instance of delay in use case implementation for the given month.
			Delay of 1 day	1	
			Delay of more than 1 day	2	
6	Security Incident Reporting to STPI	Any Severity 1 or 2 security incident detected in SOC shall be reported to concerned STPI security team **Target:** 100% of Severity 1 and 2 security incidents reported	100% of security incidents reported within	Nil	Each incident shall be reported within the given timelines

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
		within 15 minutes of each security incident detected To be calculated on per incident reporting time for each security incidents (1 and 2) reported within the given month.	the prescribed time		calculated on monthly basis and considering 24x7x365 operations.
			>97% & < 100% of security incidents reported within the prescribed time	3	
			< 97% of security incidents reported within the prescribed time	4	
7	Security and Privacy breach including Data Theft / Loss/ Corruption	Any incident where in system compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents) impacting business operations in a major way. MSP shall provide a report on the breach including remediation measures taken to mitigate the security breach. The report shall be submitted within 5 working days to STPI	No breach	For each breach/ data theft/data corruption/Data mining issue/ privacy breach, penalty will be levied as per following criteria. Any security incident detected .01% of the entire monthly	Each incident of security, data loss, data theft, data corruption or data mining shall be treated individually

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
				billing (Total Cloud platform) per month. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per quarter. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, STPI reserves the right to terminate the contract	

<table>
<tr><th>S. No</th><th>SLA Parameter</th><th>Definition & Target</th><th>Service Level</th><th>Impact Level/Penalty</th><th>Measurement Mechanism</th></tr>
<tr><td rowspan="4">8</td><td rowspan="4">Patch Management for applicable systems (Operating Systems, End-user devices, Network and Security components and tools, etc.)</td><td rowspan="4">Definition: All patches for released, to be tested for vulnerabilities, compatibility and any issues that may occur on deployment. The patch cycle shall begin from the time of release of patches, testing, approval by STPI and deployment on 100% of the target systems. The MSP shall submit a report on the completion of patch activity.
Patches shall be deployed on 100% of the system based on priority of the patches as per timelines defined below.
<table><tr><th>Priority</th><th>Timelines for complete Patch Cycle</th></tr><tr><td>Critical</td><td>1 day</td></tr><tr><td>High</td><td>3 days</td></tr><tr><td>Medium</td><td>30 days</td></tr><tr><td>Low</td><td>90 days</td></tr></table>
SLA shall be calculated on actual delay times for the complete patch cycles on a monthly basis.</td><td>100%</td><td>Nil</td><td>SLA shall be calculated on actual delay time for the complete patch cycles on a monthly basis for each patch from the date release of patch by OEM. Detailed process with stakeholder will be defined in the Operations Manual</td></tr>
<tr><td>>= 99% & < 100%</td><td>1</td><td></td></tr>
<tr><td>>= 98% & < 99%</td><td>2</td><td></td></tr>
<tr><td>>= 97% & < 98%</td><td>3</td><td></td></tr>
</table>

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
			<97%	4	Measurement shall be done for each server, node, or endpoint on a weekly basis.
9	Malware Scan	The scope includes all the servers, nodes, and endpoints both critical and non-critical. Definition: All hosts should be subjected to an anti-virus/malware scan as least once every week. Calculation: No. of servers, nodes, and endpoints for which weekly scan was run/Total count of servers, nodes, and endpoints (critical and non- critical) x100 Target: Malware scan = 100%. Devices on maintenance or are not powered up can be excluded. However, a report should be submitted on monthly basis to STPI and end customers for such devices.	100%	Nil	
			>= 99% & < 100%	1	
			>= 98% & < 99%	2	
			>= 97% & < 98%	3	
			<97%	4	

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
10	Anti-virus (AV) signature update	Availability of latest AV signature on the system components. Target: Latest AV signature to be installed on 100% of all applicable component within 24 hours. Devices on maintenance or are not powered up can be excluded. However, a report should be submitted on monthly basis to STPI and end customers for such devices.	100%	Nil	SLA shall be measured on delay of antivirus signature update in each applicable system component averaged over a monthly basis.
			>= 99% & < 100%	1	
			>= 98% & < 99%	2	
			>= 97% & < 98%	3	
			<97%	4	
11	Network and Host Intrusion prevention system – signature update	Implementation of latest NIPS and HIPS signatures on the system components. Target: Latest NIPS and HIPS signatures to be installed on 100% of all applicable components within 24 hours.	100%	Nil	SLA shall be measured on delay of NIPS and HIPS signature update in each applicable system component averaged over a monthly basis.
			>= 99% & < 100%	1	
			>= 98% & < 99%	2	
			>= 97% & < 98%	3	
			<97%	4	

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
12	System/Firmware Upgrades for all Systems – Network, Security, Storage, Centrally Managed Software Defined Solution, Servers, etc. as applicable	MSP shall upgrade the system/firmware of all applicable systems such as network components, security components and tools, storage systems and any other applicable device or tool on a half-yearly basis Target: 100% systems upgraded within the half-year as applicable	100%	Nil	SLA shall be measured on delay of firmware upgrade in each applicable system component on a half-yearly basis/
			>= 99% & < 100%	1	
			>= 98% & < 99%	2	
			>= 97% & < 98%	3	
			<97%	4	
13	Vulnerability assessment and Penetration Testing Observation Report	Vulnerability Assessment and Penetration Testing for all systems/sub systems/network devices shall be performed twice every year. VAPT observation report shall be submitted within the 30 days of the half-year period. Target: No delay	<=10 days	Nil	SLA shall be measured on delay in submission of each VA and PT observation report.
			>10 and <=20 days	4	
			>20 and <=30 days	5	
			>30 and <=35	6	
			>35days	7	

<table>
<tr><th>S. No</th><th>SLA Parameter</th><th>Definition & Target</th><th>Service Level</th><th>Impact Level/Penalty</th><th>Measurement Mechanism</th></tr>
<tr><td rowspan="4">14</td><td rowspan="4">Vulnerability assessment and Penetration Testing Closure</td><td rowspan="4">All detected vulnerabilities shall be closed by the MSPas per the below timelines and closure report shall be submitted to STPI
<table><tr><th>Vulnerability Level</th><th>Target Closure Time</th></tr><tr><td>High</td><td>Within 8 hours</td></tr><tr><td>Medium</td><td>Within one working day</td></tr><tr><td>Low</td><td>Within 3 working days</td></tr></table>
Target: 100% of vulnerabilities closed as per the above timelines (each category of vulnerability shall be treated separately for calculation of SLAs).</td><td>100% of vulnerabilities closed as per target closure time</td><td>Nil</td><td rowspan="4">SLA shall be measured for delay in closure of each vulnerability vis-à-vis target closure time. Detailed process with stakeholder will be defined in the Operations Manual</td></tr>
<tr><td><100% and >=99% of vulnerabilities closed as per target closure time</td><td>4</td></tr>
<tr><td><99% and >=98% of vulnerabilities closed as per target closure time</td><td>5</td></tr>
<tr><td><98% and >=97% of vulnerabilities closed as per target closure time</td><td>6</td></tr>
</table>

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
			<97% of vulnerabilities closed as per target closure time	7	
15	Review and Compliance to Policy, Procedure and Hardening Guidelines	Half-yearly review of compliances to policies, procedures, and hardening guidelines of deployed infrastructure in line with STPI security policies, procedures, ISO standards, security guidelines, etc. Review report shall be submitted within the next month of review exercise. Target: 100% compliance	100% compliance	Nil	SLA shall be measured for each instance of non-compliance for the corresponding half-year.
			<100% and >=99 % compliance	4	
			<99% and >=98 % compliance	5	
			<98% Compliance	6	
16	Review of security baselines configuration and configuration review of all IT infrastructure and cyber security	Review of security baselines configuration and configuration review of all IT infrastructure and cyber security components on a quarterly basis. MSP shall submit a quarterly report on the compliance to baseline configuration. Target: 100% compliance to security baseline configuration.	100% Compliance	Nil	SLA shall be measured on each instance of non-compliance to baseline configurations for the

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
	components on a quarterly basis				corresponding half-year.
			<100% and >=99% compliance	3	
			<99% and >=98%	4	
			compliance		
			<98% compliance	5	
17	MIS Report	Weekly MIS report covering the malware scanning, systems patched, and security incidents resolved, prevented attacks, tools performance, security analytics, etc. to be submitted to STPI on every Sunday for the previous week's activities. The MIS report template shall be discussed and agreed mutually with STPI. Target: No delay.	No delay	Nil	SLA shall be calculated on the basis of each instance of delay in submission of weekly MIS report. Each MIS report shall be considered individually.
			1-3 days	1	
			More than 3 days	2	
18	Security Report	Monthly security report on the security KPIs defined mutually with STPI to be submitted at the end of every month.	No Delay	Nil	SLA shall be calculated on the basis of each instance of delay

S. No	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
			1-3 days	1	in submission of monthly security report. Each security report shall be considered individually.
			More than 3 days	2	

3.17.9. SLA for Service Desk

Sno.	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
1	Availability of helpline at service desk location	Uptime = {1 – [(Helpline downtime)/ (Total Time)]} Total Time shall be measured from 7:00 am to 5:00 pm on all working days. Downtime shall be measured from the time the helpline at the service desk becomes unavailable to the STPI users/employees/stakeholders to the time it becomes available	100% uptime measured on a monthly basis	Nil	Measured for helpline availability within the defined time measured on a monthly basis.
			>= 97% to <100% up time measured on a monthly basis	3	
			>= 94% to <97% up time measured on a monthly basis	4	
			<94% up time measured on a monthly basis	5	
2			100% within the defined target	Nil	

Sno.	SLA Parameter	Definition & Target	Service Level	Impact Level/Penalty	Measurement Mechanism
	Service Desk ticket/Incident Response time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email, or ticketing tool. This is calculated for all tickets/incidents reported within the reporting month. Target: 15 Minutes	>=99% and <100% meeting the target	4	Measured for each ticket/ incident individually
			>=97% and <99% meeting the target	5	
			>=95% and <97% meeting the target	6	

3.17.10. SLA for Service Provisioning

Sno.	SLA Parameter	Definition & Target	Service Level	Impact level	Measurement Mechanism
1	Service Provisioning	Cloud platform should be able to provision any service in less than 15 minutes from the time of the request	<=15 mins	Nil	Measured for each request for provision of services
			>15 mins and <=20 mins	6	
			>20 mins and <=25 mins	7	
			>25 mins and <=30 mins	8	
			>30 mins and <=35 mins	9	

3.17.11. SLAs for CSP

The objective of this clause is to establish a mechanism for holding the Managed Service Provider (MSP) accountable for ensuring that the Cloud Service Provider (CSP) meets all the Service Level Agreement (SLA) criteria. In the event of CSP non-compliance with SLAs, the MSP shall be liable to pay penalties as outlined in this clause.

To illustrate calculation of penalties, an indicative example is provided below.

a. The payment should be linked to the compliance with the SLA metrics.

b. The penalty in percentage of the quarterly payment is indicated against each SLA parameter in the table.

    i. For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Quarterly payment is deducted from the total of the bill and the balance paid to the Service Provider
    ii. If the penalties are to be levied in more than one SLA, then the total applicable penalties are calculated and deducted from the total bill and the balance paid to the Service Providers.

c. For ex: SLA1 =7% of the quarterly payment, SLA12=10% of the quarterly payment, SLA19=2% of the quarterly payment then Amount to be paid = Total bill – {(19% of the Quarterly Payment)

In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
Availability/Uptime				
1	Availability/Uptime of cloud services Resources for Production environment	Availability (as per the definition in the SLA) will be measured for each of the	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resources will attract penalty as indicated below.

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
	(VMs, Storage, OS, VLB, Security Components,)	underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP		<99.5% &=99% (10% of the Quarterly Payment)
				< 99% (20% of the < Quarterly Payments >)
2	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / Deactivation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below.
				<99.5% & =99% (10% of the <Quarterly Payments>)
				< 99% (20% of the < Quarterly Payments >)
3	Availability of the network links at DC and DR (links at DC / DRC, DCDRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%	Default on any one or more of the provisioned network links will attract penalty as indicated below.
				<99.5% & =99% (10% of the <Quarterly Payments>)

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
				< 99% (20% of the Quarterly Payments) >
4	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate based on the audit, then this SLA is not required.	5% of < Quarterly payments >
The following SLAs apply both for CSP and MSP. While the CSP will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the MSP will be responsible for the SLAs related to managing and monitoring the cloud services				
Support Channels - Incident and Helpdesk				
5	Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15minutes	<95% & >=90% (5% of the <Quarterly Payment>) < 90% & >= 85% (7% of the <Quarterly Payment >) < 85% & >= 80% (9% of the <Quarterly Payment >)

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
6	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	<98% & >=90% (5% of the <Quarterly Payment>) < 90% & >= 85% (10% of the < Quarterly Payment >) < 85% & >= 80% (20% of the < Quarterly Payment >)
7	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting	<95% & >=90% (2% of the <Quarterly Payment>) < 90% & >= 85% (4% of the <Quarterly Payment >) < 85% & >= 80% (6% of the < Quarterly Payment >)
Security Incident and Management Reporting				

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
8	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e., month). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery	95% within 1 hour	<95% & >=90% (5% of the <Quarterly Payment>) < 90% & >= 85% (10% of the < Quarterly Payment >) < 85% & >= 80% (15% of the < Quarterly Payment >)
9	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95% & >=90% (5% of the <Quarterly Payment>) < 90% & >= 85% (10% of the < Quarterly Payment >) < 85% & >= 80% (15% of the < Quarterly Payment >)
Vulnerability Management				

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
10	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.). • High Severity Vulnerabilities – 30 days - Maintain 99.95% service level • Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level	99.95%	>=99% to <99.95% (10% of the <Quarterly Payment>) >=98% to <99% (20% of the < Quarterly Payment >) < 98% (30% of the < Quarterly Payment >)
11	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.).	99.95%	>=99% to <99.95% (10% of the <Quarterly Payment>) >=98% to <99% (20% of the <Quarterly Payment >) < 98% (30% of the < Quarterly Payment >)

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
12	Security breach including Data Theft/Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR << 5 Lakhs>>.This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << STPI reserves the right to terminate the contract.
13	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		(e.g., 3 working days from the end of the month)	5% of <Periodic Payment>
Service levels for CSP				
14	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<<RTO= 4 hours>> [STPI to indicate based on the application requirements]	10% of <Quarterly Payment> per every additional 4 (four) hours of downtime
15	RPO (Applicable when taking Disaster Recovery as a	Measured during the regular planned or unplanned	<<RTO= 2 hours>> [STPI to indicate based	10% of <Quarterly Payment> per every additional 2 (two) hours of downtime

Sr. No.	Service level objective/criteria	Measurement Methodology	Target/Service Level	Penalty (Indicative)
	Service from the Service Provider)	(outage) changeover from DC to DR or vice versa.	on the application requirements]	
16	Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		Average within 5 Working days	5% of <Quarterly Payment>

Note:

1. Availability is defined as:
   {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%
2. Cloud “Service Level Objective” (SLO) means the target for a given attribute of a cloud service that can be expressed quantitatively or qualitatively.
3. Response time is the time interval between a cloud service customer-initiated event (e.g., logging of the request) and a cloud service provider-initiated event in response to that stimulus.
4. “Scheduled Maintenance Time” shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of the Department, during non-business hours. The Scheduled Maintenance time <> as agreed shall not be considered for SLA Calculation.
5. “Scheduled operation time” means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.
6. “Availability” means the time for which the cloud services and facilities are available for conducting operations on the Department system. Availability is defined as: {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%
7. “Incident” refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the cloud consumer to the Cloud Service provider (CSP) can be termed as an Incident.

3.17.12. Liquidated Damages

i. The Service Level Agreement (SLA) reconciliation shall be conducted on a yearly basis to assess the performance of the Managed Service Provider (MSP) and ensure compliance with the agreed-upon SLA metrics

ii. SLA penalties during the operations phase (Post Go-Live) shall be calculated on a monthly basis and will be deducted quarterly from the applicable payment.

iii. Monthly MIS report shall be submitted by MSP covering all the key details, SLA compliance of all the functions as per **Section 3.17**.

iv. STPI can prescribe specific periods when the system should be available 100% and if the system does not meet SLA, 2x SLA penalties will be charged for that month in which the system does not meet the SLAs for the prescribed period.

v. Each SLA as mentioned above is independent and accordingly the penalties shall be calculated

Note:

a) The onboarded MSP must ensure that the project's uptime and performance requirements, as stated in the Service Level tables above, are met. If any upgrades or significant changes are made to the infra setup, the MSP must plan them accordingly to ensure compliance with the Service Level requirements and take approval from STPI.

b) Any differences or inconsistencies in a Service Level will not impact the MSP's responsibilities to deliver the Services as per the Agreement and strive to meet or surpass the specified service standards

vii. The MSP can be a Cloud Service Provider (CSP) empanelled with MeitY or an authorized partner/reseller/distributor of the MeitY empanelled CSP. The CSP would be responsible for the following:

a. Resource commitment - CSP will place key project management, cloud architects and technical support professionals for entire duration of the project. CSP resources should not be less 10% of overall project resources (CSP & MSP together) at any point in time in the project duration.

b. Right pricing of services - CSP would be responsible for offering competitive rates for IaaS/PaaS/SaaS services. This is very important for success of this hybrid cloud and GCC project.

c. Project governance – CSP is equally responsible for the success of the project for success.

   I. Architecture governance – quarterly review

   II. Customer escalations – handle customer escalations in timely and effective manner to help MSP address the technical issues efficiently.

   III. Customers add/churn progress monitoring and joint planning to retain the customer

d. CSP should help the project in lead generation and sales pipeline creation activities, conversion of leads would be MSP responsibilities. MSP, CSP and STPI would do a monthly review on leads conversion, challenges and help required etc

3.18. Make in India (MII)

The bidder shall ensure the "Make in India" initiative guidelines of Department for Promotion of Industry and Trade, Ministry of Commerce and Industry vide order no. P-45021/2/2017-PP (BE-II)

Section IV: Scope of Work

4.1. High level overview

1. The MSP shall setup and manage the Hybrid Cloud at STPI Data Centres for offering Cloud services (Cloud services offerings as per Annexure-G) from at least five locations. Currently available locations are as following:
   i. Bengaluru
   ii. Mohali
   iii. Bhubaneshwar
   iv. Chennai
   v. Vijayawada
2. The MSP shall setup & manage Government Community Cloud (GCC) services (Cloud services offerings as per annexure G) from at least two of the above stated STPI Data Centres.
3. Indicative Cloud service deployment models to be offered by the MSP are provided as below,
   - Infrastructure as a Service (IaaS)
   - Platform as a Service (PaaS)
   - Software as a Service (SaaS)
4. MSP shall also offer professional services from this project such as (may not limited to) building captive Data Centre, Backup and DR as a service, DevOps as a Service etc These services will be incorporated into the service catalogue as available options
5. The MSP shall manage the Hybrid Cloud and Government Community Cloud (GCC) setup for the contractual period at existing STPI Data Centres.
6. The MSP shall be working as an advanced services cloud partner of STPI in revenue sharing model for which the MSP shall be given a free hand to market and sell the cloud services in partnership with STPI. Both STPI and MSP shall target to achieve the operational efficiency of Data Centres to increase the sales and revenues.
7. The MSP shall deploy and commission complete setup with minimum nodes/Systems from go live date so that STPI should be able to offer the minimum Services volume mentioned in the **Annexure G.**
8. All the Investment required to setup the Hybrid Cloud and Government Community Cloud (GCC) setup shall be borne by MSP excluding the STPI Obligation.
9. MSP to provide a complete IT platform with agility and reliability via advanced cloud services (IaaS, PaaS, SaaS) to the start-ups, Enterprises and Govt. departments.
10. Facilitate the Start-up ecosystem by hosting digital products on STPI platform at single marketplace.
11. Leveraging at least seven of the edge Data Centre locations of STPI for providing applicable cloud services as per proposed edge location utilization plan.
12. Public & Private Partnership (Revenue sharing) to capitalize the industry expertise.
13. Establish STPI as a leading player Cloud services to serve Indian and offshore clients.
14. The MSP shall bring bouquet of cloud services which shall be offered from STPI Data Centres in hybrid mode thus maximizing the revenue per sq.ft./ per KW from STPI Data Centres.
15. The MSP shall offer advanced cloud services (IaaS, PaaS, SaaS) and Hybrid Cloud services from all existing STPI Data Centres, which may be extended to the new facilities when they are ready.
16. The MSP shall be responsible for the MeitY empanelment of STPI Data Centres.

Note: Mohali and Bangalore DC locations are operated and managed by a third-party vendor on PPP model. The GCC infra (if required) may be deployed at these locations based on the demand of business and terms of deployment will be decided mutually.

An indicative and high-level view of the transformed STPI Data Centres is illustrated in figure below:

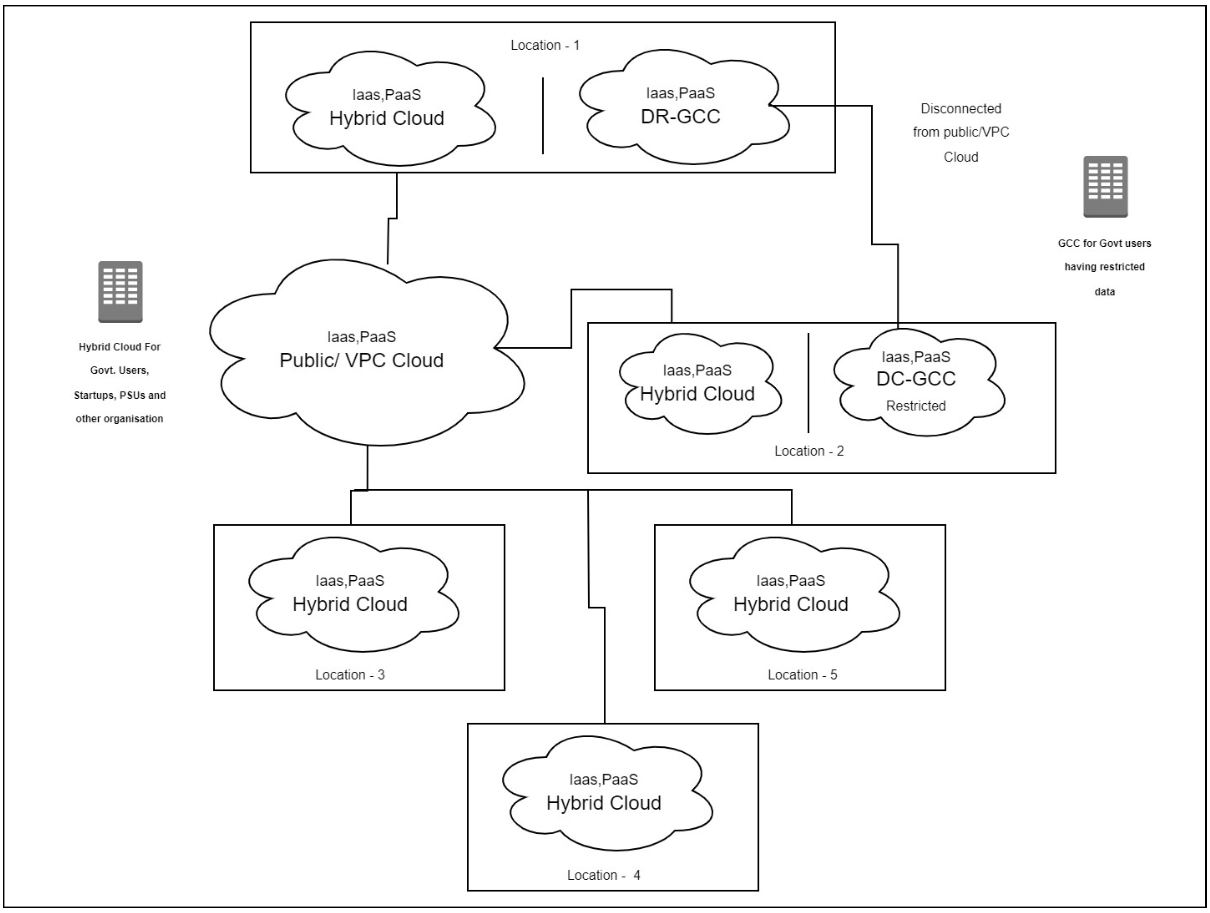


Figure 1 – High level view of transformed STPI Data Centres

Following sections details the scope of work to be undertaken by the successful MSP for providing the advanced IaaS including hybrid, PaaS and SaaS services from STPI Data Centres.

4.2. Hybrid Cloud setup and Management

The Hybrid Cloud is a composition of On-Premises and Public Cloud, and integration between the clouds which remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.

True hybrid environment deliver consistency across all Data Centres and cloud environments by which Users/Customers can continue to leverage their existing infrastructure and share data seamlessly across platforms, easily integrating with next-generation services and innovating rapidly.

The MSP shall ensure that by using STPI Hybrid Cloud environment the organizations must be able to build and deploy innovative applications using a consistent framework, processes, and tools across

Public Cloud and Hybrid Cloud (STPI DCs). MSP shall be following the key guiding principles for STPI Hybrid Cloud:

A. **Control deployment options for their applications:** Developed applications should follow the same approach for all the Data Centres (Hybrid or Public Cloud) so that they are easily deployed to either location based on required regulations and the need to protect sensitive data, customization, and latency.

B. **Keep application data where it belongs to:** In Public Cloud, Data Centres must be adhering to stringent security and privacy regulations, or the data must reside in the own Data Centres of Government departments.

C. **Get to market and address business needs faster:** The new application development should be facilitated by leveraging on application components selected from Solution Catalogues.

D. **Efficiently deploy and manage the infrastructure:** Deployment should be fast, and the infrastructure must be in position to scale over time as business needs changes. Also, the user organizations/departments must be in position to leverage a unified management solution, to guarantee the protection and disaster recovery of applications and workloads.

E. **Move to a pay-as-you-use approach:** Proposed Hybrid Cloud shall allow Customers to use a variety of Services and pay only for what they use.

The MSP Shall ensure:

a) The minimum configured cloud services will be as per **Annexure-G.**
b) These services shall be always compliant to MeitY guidelines as released from time to time.
c) These services shall be published through a STPI's Cloud Services Directory for use by government departments or agencies at the Centre and States.
d) The MSP shall ensure that services offered by CSP should be in consonance with MeitY cloud service bouquet. CSP shall adhere to any changes or any update in MeitY service bouquet.

4.2.1 Infrastructure as a Service (IaaS)

The capability shall be provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include the operating systems and applications. The consumer shall not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls).

4.2.2 Platform as a Service (PaaS)

The capability shall be provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but shall have control over the deployed applications and possibly configuration settings for the application hosting environment.

4.2.3 Software as a Service (SaaS)

The capability shall be provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user specific application configuration settings.

4.2.4 Connecting STPI Hybrid Cloud and Public Cloud resources

Hybrid environments natively integrate with Public Cloud environments, enabling consistent connections to cloud across identity, subscription, billing, backup and disaster recovery, including catalogue of services provided. It would also enable Government departments to seamlessly use and move amongst public, government-only, and on-premises cloud environments to rapidly respond to geopolitical developments and cybersecurity threats. A Hybrid Cloud enabling infrastructure shall be composed of but not limited to the following:

- Hybrid Cloud deployed on a scalable architecture hosted in the STPI Data Centre, offering a specific set of Services mentioned in the RFP.
- Public Cloud, adhering to stringent security and privacy regulations, offering an extensive set of services mentioned in the RFP
- Seamless connectivity and Integration between the Hybrid Cloud and the Public Cloud.

The MSP shall provide in its solution, the required infrastructure (e.g. VPN) for connecting Hybrid Cloud from STPI DC and Public Cloud resources via a secure tunnel to facilitate the creation of a single enterprise environment.

Hybrid Cloud → internet link(s) → Public Cloud

The secure tunnel shall be set up by the MSP. Internet access (to connect Cloud) shall be provided by STPI and will be on chargeable basis as per the STPI rate card.

The MSP shall provide the customised cloud management layer which can integrate with Public Cloud, Hybrid Cloud (Via STPI DCs) and any other integration point.

4.2.5 Hybrid Cloud from STPI Data Centres

A dedicated multi-tenant Cloud consisting of compute, network and storage . Hybrid Cloud shall provide consumer level access to infrastructure usage and computational resources. The list of required services is provided in **Annexure G.**

4.2.6 Public Cloud part of Hybrid Cloud (Extension)

The Hybrid Extension part of the infrastructure enabling interoperability with external resource providers shall be an open, flexible, enterprise-grade Cloud Computing platform, which will support all infrastructure, platform and software requirements coming from the Government. The Hybrid Extension should be based on a shared multi-tenant infrastructure in which the cloud infrastructure and computing resources are made available to the government users over a virtual public network and is owned by the Cloud Provider. The list of required services is provided in **Annexure G.**

4.2.7 Indicative deployment of Solution for Hybrid Cloud

A. Hybrid Cloud environment shall be operational with minimum 1 number of 42U racks covering Network, Storage, Compute and Security components. It shall have minimum 2 nodes deployed in the beginning with capability to scale as per future demand. Each node shall consist of but not limited to the following requirements:

   I. Minimum usable physical cores/node – 56

   II. Physical to virtual core ratio - 1:2

   III. Minimum raw storage/node – 250 TB (it should be appropriate mix of NVMe, SSD, HDD)

   IV. Minimum memory /node – 2.8TB

   V. Hybrid environment shall be capable enough to scale as per the demand.

B. The requirements mentioned above are for initial setup only. Based on the growth of project, the solution shall have the capability to scale up within rack as well as in multiple racks.

C. The MSP shall purchase additional nodes/racks as required. All information supplied by the MSP shall be treated as contractually binding on the bidders on successful award of the assignment by STPI based on this RFP.

STPI may include upcoming datacentre facility under the same term & conditions of the contract against this RFP with mutual agreement.

4.4. Setup of Government Community Cloud

The MSP shall setup Government Community Cloud (GCC), as per MeitY guidelines, at 2 number of Data Centre facilities of STPI with minimum 10 racks each and manage as per the timeline mentioned in this RFP (Section 4.29).

The GCC setup shall be carried out at STPI’s Bhubaneshwar and Vijayawada locations. It is important to note that these locations are currently identified as tentative and subject to change during the implementation phase.

The MSP shall ensure that the GCC setup must be always compliant to MeitY guidelines.

Few of the key clauses of MeitY guidelines are mentioned below for bidder’s reference.

GCC related Clause in MEITY Empanelment *
GCC Definition by MEITY: The infrastructure elements including physical server, physical storage (including backup storage) and network infrastructure of the Government Community Cloud should be dedicated to the Government Department solutions and be physically separate from the public and other cloud offerings of the Cloud Service Provider. There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications, and servers. However, the dedicated infrastructure elements can be shared by the Government Departments.
Must have Separate VLAN provision with dedicated firewall between the VLANs and for each and every client on the dedicated Government Community Cloud.
The management consoles for the dedicated Government Community Cloud should only show the data for the dedicated Government Community Cloud and in the same manner, the monitoring data of the dedicated Government Community Cloud shall not be available on any other management console.
Security toolset, except DDOS, shall be a dedicated installation of the tools / products for the Government Community Cloud. DDOS need not be a dedicated installation for the Government Community Cloud and may be deployed as a shared service.
GCC related Clause in MEITY Empanelment *
For ensuring strategic control of the operations, approval of the MeitY/Government Departments shall be taken prior to making changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud. The above set of activities where prior approvals of the MeitY have to be taken is only indicative and by no means an exhaustive list. The set of activities for which such approval has to be obtained will be finalized by MeitY/Government Department and reviewed on as needed basis.

The Government Community Cloud, MeitY and Government Department reserves the right to verify the infrastructure.
Setup the Governance Structure to review and approve changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc of the dedicated infrastructure and solutions of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud
Dedicated infrastructure for GCC, physically isolated from Public Cloud, minimum 10 racks as per latest guidelines

* *Above clauses are mentioned for a high-level understanding purpose only. Bidder need to refer the latest GCC definition and clauses. Bidder may refer the www.miety.gov.in. and comply with relevant clauses*

The MSP shall also ensure that the entire GCC infrastructure to be audited/certified by the STQC for MeitY empanelment and get the GCC status for the proposed GCC infrastructure.

4.4.1 GCC network

It is essential to design GCC network as per MeitY guidelines. As per MeitY guidelines for government customers would adopt GCC if:

I. Due to Regulatory requirements in case physical segregation of application/infrastructure is required from enterprise network, Department may choose Government community cloud (GCC) model.

II. If Physical Hardware Appliance such as firewall/HSM/Storage is a necessary requirement Department may choose Government community cloud (GCC) model.

4.5 Deployment of Centrally Managed Software Defined Solution

The Hybrid Cloud solution shall be a mix of private cloud at STPI and Public Cloud services. The non-Public Cloud part of the Solution will be based on a centrally managed software defined solution as per deployment stated below:

S. No	STPI DC location	Hybrid Cloud setup	GCC Setup
1.	Bhubaneshwar	At least 5 locations	Any two locations
2.	Mohali		
3.	Bengaluru		
4.	Vijayawada		
5.	Chennai		

4.6 Indicative deployment of Solution for GCC environment

A. The MSP shall ensure that GCC environment is operational with minimum 10 numbers of 42U racks covering Network, Storage, Compute and Security components. It shall have minimum one cluster with 16 nodes deployed. Each node shall consist of but not limited to the following requirements:

I. Minimum physical cores/node – 56

II. Physical to virtual core ratio - 1:2

III. Minimum raw storage/node – 250 TB (it should be appropriate mix of NVMe, SSD, HDD)

IV. Minimum memory /node – 2.8TB

V. GCC environment shall be capable to scale as per the demand.

Above deployment requirements are indicative and actual minimum required infrastructure should be considered as per the GCC guidelines.

4.7 BYOL- Bring your own Licenses

1. The MSP shall provide the option for the customer to use their own software licenses in the data Centre.
2. The MSP shall ensure that all hardware and software requirements for the customer's licensed software are met.
3. The MSP shall not be responsible for any issues or problems arising from the use of the customer's licensed software, and the customer shall indemnify the MSP against any such issues or problems.
4. The MSP shall provide technical support for the data Centre infrastructure only and shall not provide technical support for any third-party software or licenses used by the customer."

4.8 Implementation of Tailored Managed and Professional services

1. Scope of Services: Define the scope of services that the MSP will provide, including the specific managed services and professional services that will be tailored to the organization's unique needs.
2. Service Level Agreements (SLAs): Specify the SLAs that the MSP must adhere to, including uptime, response times, and resolution times. These SLAs should be tailored to the organization's specific needs.
3. Reporting: Specify the types of reports and data that the MSP will provide to the organization, including performance metrics, incident reports, and status updates. These reports should be tailored to the organization's specific needs.
4. Change Management: Describe the MSP's process for managing changes to managed services and professional services, including the process for requesting, approving, and implementing changes. This should also include a description of the MSP's change management tools and processes.
5. Training: Specify the training that the MSP will provide to the organization's staff on the tailored managed services and professional services. This should include a description of the MSP's training materials, methodologies, and delivery methods.
6. Pricing: Provide a pricing structure that reflects the tailored nature of the managed services and professional services. This should include a description of any additional costs associated with customization and any discounts or incentives for long-term contracts.

4.9 Implementation of Captative Data Centres

The onboarded MSP shall offer the services for implementation of Captive Data Centres including planning, designing, construction and delivery. Which may be offered as system integration services for captivate Data Centres required for the exclusive client needs e.g. Govt. departments/PSUs with critical information.

4.10 Implementation of Data Classification at STPI data Centre:

The selected MSP will be responsible for conducting the data classification exercise to categorize and classify the data assets of the organization in line with the standards and regulations specified by the NCIIPC.

- The MSP shall work closely with STPI to understand their data protection requirements and ensure that the data classification exercise is aligned with their specific needs.
- The MSP shall ensure that the data classification exercise is carried out in a secure and confidential manner, with appropriate controls in place to safeguard the sensitive information.
- The MSP shall provide STPI with clear and concise documentation outlining the results of the data classification exercise, including a comprehensive report with recommendations for the appropriate security controls and measures to be implemented.

4.11. Escalation Matrix

The MSP shall define and submit an escalation matrix for handling security risks and incidents. The escalation matrix shall clearly define the following:

A. Escalation team members and their roles and responsibilities within the escalation matrix.
B. Identify and define risk and severity levels for reporting and action
C. Update escalation matrix on need basis in case there are changes to team member roles.

4.12. MeitY empanelment of STPI Services

A. MSP shall ensure to empanel STPI as Cloud Service Provider (CSP), including but not limited to the following:

   I. MSP shall submit the application to empanel STPI as CSP at MeitY. The MSP shall fulfil all the compliance requirements mandatory for the MeitY empanelment with the assistance of STPI.

   II. The application shall be submitted to MeitY in T+3 months as per **Section 4.29**

   III. Proposed IaaS, PaaS, SaaS services from STPI Data Centres shall be empanelled with MeitY, following the guidelines by the bidder on regular basis.

   IV. The GCC offering from STPI Data Centres shall also be certified by MeitY/MeitY appointed auditors, which will be taken care by the MSP.

B. The MSP shall be responsible for Re-certify the services and CSP empanelment by MeitY during the contract period, as and when applicable.

C. The MSP may plan for site visit of proposed GCC Data Centre locations of STPI before submission of bid and provision for all costs associated with MeitY empanelment including gap in Data Centre certifications, if any.

4.13. Customer acquisition

A. The MSP would act as a cloud partner of STPI in revenue sharing model. MSP would be given a free hand to market and sell the cloud services in partnership with STPI. All parties i.e. STPI, MSP and CSP will target to increase the sales & revenues and work towards increase in consumption of IaaS, PaaS, SaaS and other cloud services from Hybrid Cloud setup and GCC.

B. MSP may setup a dedicated sales/marketing team with presence in multiple geographies for continuous revenue generation. As part of this team, it is important to deploy experienced professionals who are experts in selling IaaS, PaaS, SaaS and other cloud services and have decent understanding of how government departments and procurement system works.

C. It is also important to setup a services team to ensure end-customer technical needs are covered and there is stickiness of customer with STPI Hybrid Cloud setup. MSP would ensure that customer churn is minimum.

D. The size of sales & services team of MSP might be small in beginning which should scale up as per the requirements.

E. MSP and CSP should ensure that the additional value-added services may be provided for early cloud adoption and maintaining customer win rate, for example:

I. Migration of customer's existing application workload to STPI Hybrid Cloud environment
II. Managed service for customer application maintenance
III. Any additional development/cloudification/code change to suit cloud adoption
IV. Full migration testing including penetration testing etc.

F. A steering committee having representation from STPI, MSP and CSP shall be setup with a constant endeavour for bringing more customers, increase in customer satisfaction and generating more revenue from this setup. All parties shall be responsible for success of this project. Steering committee would meet once in every month of first 2 years of project and then once in every quarter.

4.14. Customer churn situation

A. STPI or MSP shall not suspend the right to access or use the Cloud Services without providing a written notice, 30 days in advance, to the customer, unless the use of the Cloud service offerings by the customer poses a security risk to the Cloud Services being consumed by the customer.

B. MSP shall not delete any data at the end of the end user agreement from the underlying CSP's Cloud environment (for a maximum of 45 days beyond the expiry of the end user agreement) without the express approval of the end user. The end user shall pay to the MSP the cost associated with retaining the data beyond 30 days.

C. MSP shall be responsible for providing the tools for import / export of VMs, associated content, data, etc., and MSP, in consultation with the STPI and end customer, shall be responsible for preparation of the churn management plan and carrying out the churn management / transition related activities.

D. MSP may provide a value-added service for following activities:

I. Transition of Managed Services from STPI cloud environment to new environment

II. Migration from the STPI cloud environment to the new environment

E. MSP shall always ensure that all the documentation required by the end customer for smooth transition (in addition to the documentation provided by the underlying CSP) are kept up to date and all such documentation is handed over to the customer during regular intervals as well as during the exit management process

4.15 Project Ownership

4.15.1. IT infrastructure

The IT infrastructure (Hardware, Networking devices etc.) for Hybrid Cloud and GCC environment shall be as following:

I. MSP shall purchase IT infrastructure in their own name and deploy in STPI Data Centres as per proposed plan. MSP shall provide actual purchase cost to STPI during entire project period for IT infrastructure deployed.

II. The MSP shall keep an up-to-date inventory of IT assets for GCC & Hybrid Cloud and shall submit fortnightly asset deployment report to STPI.

III. STPI would enable necessary racks space with required power for the project, MSP shall pay rack space power cost to STPI as per prevailing tariff.

IV. As GCC and Hybrid Cloud Data Centres might contain important government information therefore it will be important for the MSP to ensure all security and sanitization checks before IT infrastructure is commissioned for the project.

V. In case of contract termination, section 3.15 (Termination) will be applicable.

VI. MSP shall plan to refresh the end-of-life IT infrastructure as and when end-of-life period is reached of deployed infrastructure.

4.15.2. Subscription on Cloud for customer in Hybrid cloud environment

I. MSP and CSP shall device and publish cloud subscription along with rates for Hybrid Cloud Services and GCC services including all IaaS, PaaS, SaaS services. The service offerings must be in-line with MeitY Cloud services bouquet document.

II. Creation of customer tenants on hybrid and GCC cloud would have overall ownership of STPI, and these tenants shall be managed by the MSP for the contract duration.

III. MSP shall be responsible for sharing the deployment details with STPI and CSP on a fortnightly basis. The reporting mechanism could be jointly decided at the beginning of the project.

4.15.3. Network bandwidth

I. STPI itself being a Class ‘A’ ISP provides bandwidth to its Data Centres, therefore the MSP shall have to procure network bandwidth from STPI only.

II. MSP shall be responsible for meeting the SLA requirements for performance and availability by provisioning sufficient internet connectivity at each Data Centre for Hybrid Cloud and GCC operations. MSP must have to keep enough bandwidth for the DC-DR operations.

III. In the event of failure of GCC Data Centre, the MSP is responsible for Disaster Recovery (DR) Services to ensure continuity of business operations while meeting the RPO and RTO requirements. RPO and RTO for Disaster Recovery & Business Continuity Requirements shall be as per MeitY guidelines as following:

   A. RPO shall be less than or equal to 15 minutes.
   B. RTO shall be less than or equal to 60 minutes.
   C. MSP shall always adhere to RPO and RTO guidelines defined by MeitY during the contract period.

IV. For calculation & bid submission purpose, the MSP may assume the minimum bandwidth requirement of 1Gbps internet connectivity at each Data Centre for Hybrid Cloud and GCC operations and 155Mbps link for DC-DR.

V. STPI shall enable necessary bandwidth for the project, for which the MSP shall pay network bandwidth cost to STPI as per prevailing tariff of STPI. The tariff will be decided by the STPI.

4.15.4. Monitoring of services

MSP and CSP will both have regular sync on customers provisioned, optimization required for customer workloads etc.

4.15.5. CSP obligations

The CSP shall be responsible for the following, but not limited to:

1. The cloud infrastructure and all STPI and User data must be hosted and maintained in India only. Any STPI data cannot be moved to other site without prior written approval from designated authority by STPI.
2. STPI shall have right to scale horizontally and vertically as per the user workload requirement and applications compatibility. There shall be a provision for auto scaling as per the user requirement.
3. CSP shall provide detailed audit trail reports for portal login, enabling administrators to identify all actions taken through the cloud portal / API. It should also provide a variety of usage reports that enable administrators to identify historical service usage. Every activity undertaken under admin access should be logged and the same to be communicated to STPI.
4. During the Term, new cloud services and /or features may be available as a result of technology advancement, the CSP shall keep informing STPI to update the service catalogue.
5. CSP shall not publish or disclose any information in any manner related to this project, without STPI's written consent, the details of any safeguards either designed or developed by the CSP under the agreement or otherwise provided by STPI.
6. CSP shall provide user level / user group level auditing of all administrator activities performed by STPI / STPI's vendors etc. and provide information like "but not limited to" monitoring, metering, allocation, quota / limits etc. CSP should allow STPI to download copies of these audit logs and reports in mutually agreed pre-defined format without additional charges.
7. STPI should have the right to perform Penetration Test and will notify the CSP in advance regarding the same. If STPI exercises this right, the CSP shall allow STPI's designated third party auditors to conduct required activities, to ensure all the compliances as defined by MeitY for Cloud Services offered by CSP and the security guidelines as defined by STQC are met by the CSP.
8. Providing services on a highly secure and controlled platform and providing a wide array of security features customers can use.
9. There are a lot of Security tools offered by the CSP, like:
   a. Identity and Access Management (IAM)
   b. Multi-Factor Authentication (MFA)
   c. Encryption of data associated with VM
   d. DDoS Protection
   e. TSL/SSL Certificate Management

4.15.6. Billing ownership

I. Billing will be done by STPI.

II. The reconciliation of revenue sharing between STPI and MSP shall be done on a "Quarterly" basis. STPI and MSP may invoice the other party depending on their due revenue share post reconciliation every quarter.

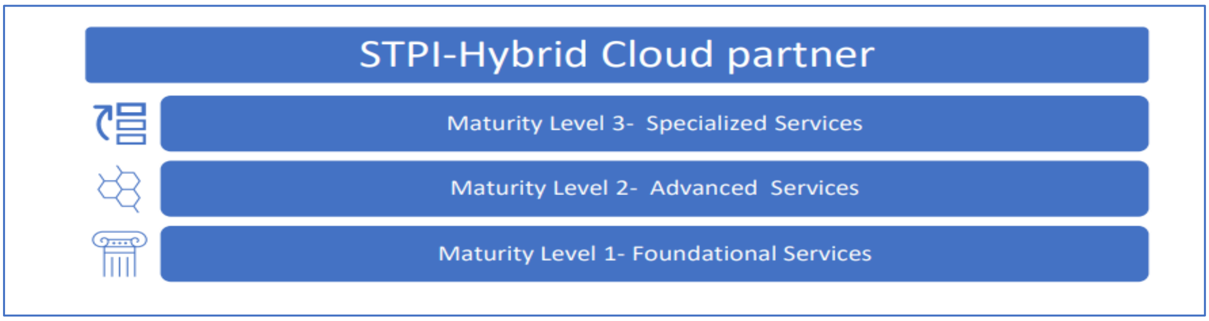
III. Taxes would be on actuals and would not be calculated for revenue calculation. Each party will be responsible for their tax obligations.

IV. MSP shall extend all possible support in generation of monthly/quarterly bills for end customers.

V. Revenue, collection activities etc. shall be managed by MSP.

4.16. Service Deployment View

Hybrid Cloud partner would have to deploy types of services depending on their project plan. STPI Hybrid Cloud maturity level will be decided based on number of services and type of services deployed by MSP. As STPI key goal for this RFP is to maximize the revenue per sq. ft of STPI Data Centre, It is expected that MSP should be choosing a capable CSP who can provide all the following services from the start date itself. The bidder has to provide the following services in the table given below.


STPI-Hybrid Cloud partner
Maturity Level 3- Specialized Services
Maturity Level 2- Advanced Services
Maturity Level 1- Foundational Services

Services	Brief Description	Service Model	Service Maturity Level
Core Infrastructure	Virtual Machines	IAAS	Level1: Foundational Services
	Serverless	IAAS	Level1: Foundational Services
	Container as Service	IAAS	Level1: Foundational Services
	Managed Database as Service (SQL Server, NoSQL)	PAAS	Level1: Foundational Services
	Storage as a Service	PAAS	Level1: Foundational Services
	Backup as a Service	PAAS	Level1: Foundational Services

Services	Brief Description	Service Model	Service Maturity Level
Network Services	DR as a Service	IaaS	Level1: Foundational Services
	Virtual Network	IaaS	Level1: Foundational Services
	Application Load Balancer	IaaS	Level1: Foundational Services
	Network load balancer	IaaS	Level1: Foundational Services
	VPN gateway	IaaS	Level1: Foundational Services
	Firewall	IaaS	Level1: Foundational Services
	Public IP	IaaS	Level1: Foundational Services
	Web Application Firewall	IaaS	Level1: Foundational Services
	Content Delivery Network	IaaS	Level1: Foundational Services
Security Services	Distributed Denial of Services	IaaS	Level1: Foundational Services
	Cloud based Hardware Security Module	IaaS	Level1: Foundational Services
	TLS / SSL Certificate Management	IaaS	Level1: Foundational Services

Services	**Brief Description**	**Service Model**	**Service Maturity Level**
	Identity and access management	PaaS	Level1: Foundational Services
	Dual / Multifactor Authentication	IaaS	Level1: Foundational Services
	Email Gateway Security as a Service	SaaS	Level3: Specialized Services
	End-Point Threat Detection & Response for Productivity	SaaS	Level3: Specialized Services
	Unified End Point Security platform	SaaS	Level3: Specialized Services
	Secure Desktop OS as a Service for enterprise users	SaaS	Level3: Specialized Services
Enterprise Management Support Services	Operational Metric Collection	IaaS	Level1: Foundational Services
	Alarm Service	IaaS	Level1: Foundational Services
	Email /SMS/Voice Call Notification Service	IaaS	Level1: Foundational Services
	subscription management support	IaaS	Level1: Foundational Services
	Log Analyzer	IaaS	Level1: Foundational Services
Application Development Services	DevOps as a Service	PaaS	Level2: Advanced Services

Services	Brief Description	Service Model	Service Maturity Level
	Low Code Application Development	PaaS	Level2: Advanced Services
	Workflow & Integration as a service	PaaS	Level2: Advanced Services
	API Management as a Service	PaaS	Level2: Advanced Services
	Application Platform (App Platform) as a Service	PaaS	Level2: Advanced Services
Data Analytics and AI/ML services	Big Data Analysis as a Service	PaaS	Level2: Advanced Services
	Data Warehouse as a Service	PaaS	Level2: Advanced Services
	Data Integration Platform as a Service	PaaS	Level2: Advanced Services
	Cognitive Services (Computer vision, Language Translation API, Search, Machine learning)	PaaS	Level2: Advanced Services
	IoT Platform as Service	PaaS	Level2: Advanced Services
	Business Intelligence & Data Visualization as a service	PaaS	Level2: Advanced Services
	Video Streaming Service	PaaS	Level2: Advanced Services
	Data Streaming Service	PaaS	Level2: Advanced Services
	Massive Data Processing Services	PaaS	Level2: Advanced Services

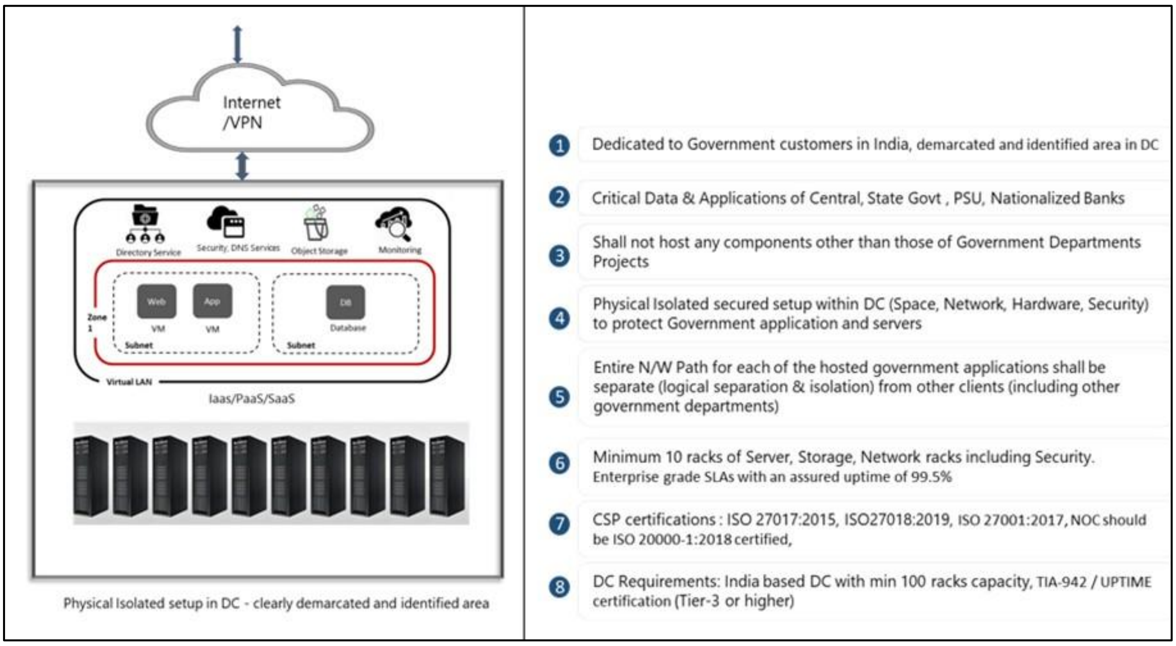
Services	Brief Description	Service Model	Service Maturity Level
Productivity apps, such as email, collaboration, and calendaring	Email, calendar and contacts	SaaS	Level3: Specialized Services
	Collaboration	SaaS	Level3: Specialized Services
	Project management	SaaS	Level3: Specialized Services
	Personal document storage as service	SaaS	Level3: Specialized Services
SaaS based COTS Business applications for small/medium enterprises, organizations	Citizen/Customer relationship case management	SaaS	Level3: Specialized Services
	Customer Insights	SaaS	Level3: Specialized Services
	Field Service	SaaS	Level3: Specialized Services
	Remote Assist	SaaS	Level3: Specialized Services
	Sales	SaaS	Level3: Specialized Services
	Marketing	SaaS	Level3: Specialized Services

4.17. Network Deployment View

There are 2 types of network deployments in this project

1. Setup of GCC network including DC-DR setup .
2. Network connectivity with CSP cloud for Hybrid Cloud setup from multiple Data Centres (Mohali, Bhubaneshwar, Bengaluru, Chennai etc.)

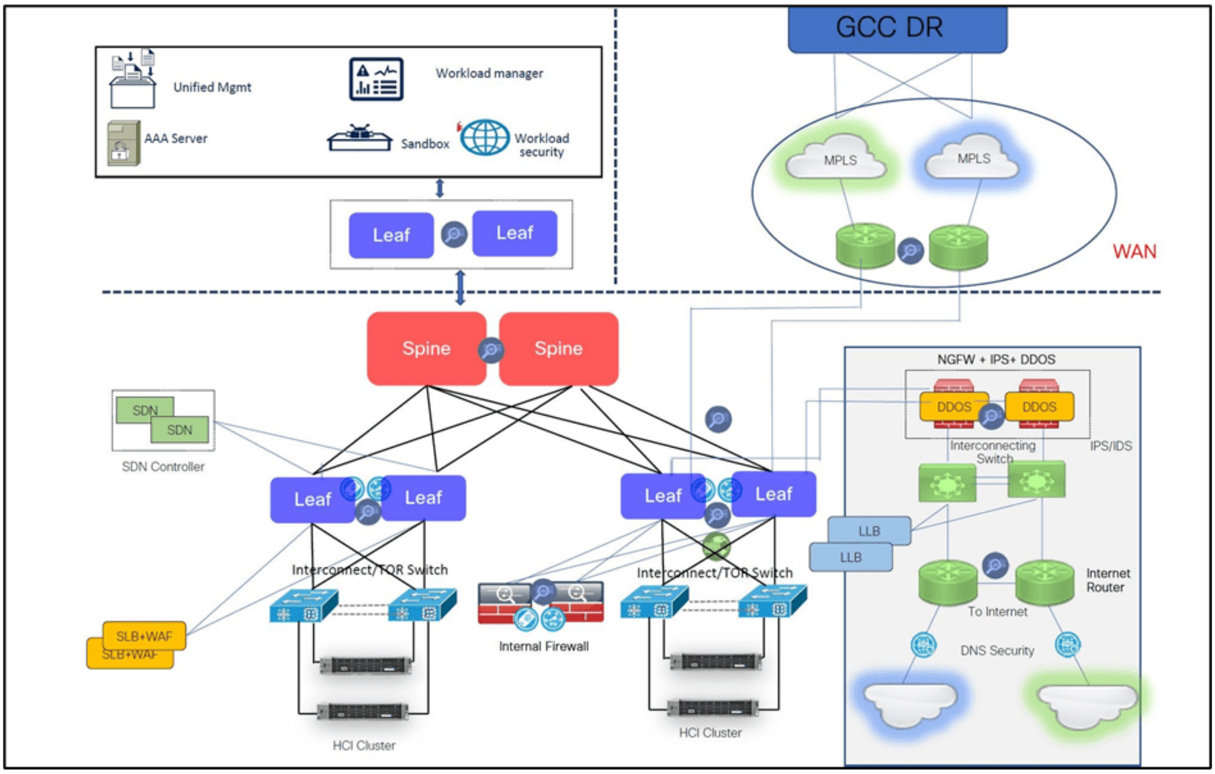
3. Logical view of GCC along with network along with is illustrated below. MSP is expected to design GCC architecture in compliance with MeitY guidelines and ensure to be compliant throughout the project lifecycle.



Physical Isolated setup in DC - clearly demarcated and identified area

1. Dedicated to Government customers in India, demarcated and identified area in DC
2. Critical Data & Applications of Central, State Govt , PSU, Nationalized Banks
3. Shall not host any components other than those of Government Departments Projects
4. Physical Isolated secured setup within DC (Space, Network, Hardware, Security) to protect Government application and servers
5. Entire N/W Path for each of the hosted government applications shall be separate (logical separation & isolation) from other clients (including other government departments)
6. Minimum 10 racks of Server, Storage, Network racks including Security. Enterprise grade SLAs with an assured uptime of 99.5%
7. CSP certifications : ISO 27017:2015, ISO27018:2019, ISO 27001:2017, NOC should be ISO 20000-1:2018 certified,
8. DC Requirements: India based DC with min 100 racks capacity, TIA-942 / UPTIME certification (Tier-3 or higher)

Illustrative deployment architecture for GCC as shown below:



4.18. Hybrid connectivity

a. IPsec site-to-site VPN connection

b. The on-premises VPN gateway device must have a public address and must not be placed behind a NAT device.

c. Multiple subnets would be required for accounting purpose

d. All clients that need to connect to parts of the service that are hosted in the Public Cloud infrastructure provider's network will need to do it from within the confines of the corporate network.

e. Use an external network load balancer to perform

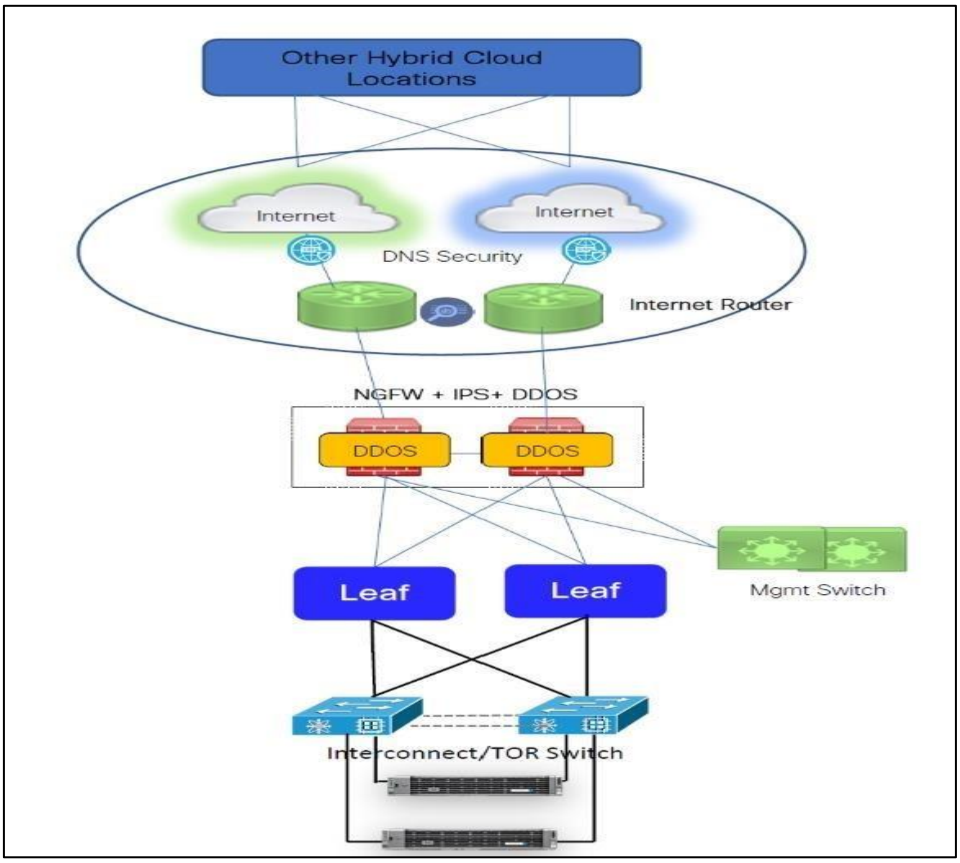
f. Load balancing of the incoming connections to the service components that are hosted in the Public Cloud infrastructure provider's network

g. Bidder will be deciding on Network load balancing requirements. Load Balancing Mechanism Provided by the Public Cloud Infrastructure Service Provider may be used. However, the need of external load balancer would be assessed by bidder in the project and accordingly to be procured.

h. Name Resolution Services Provided by the Public Cloud Infrastructure Service Provider.

i. Top of Rack/Interconnect switch for connectivity between of Centrally Managed Software Defined Solution farms.

Illustrative deployment architecture as shown below:



4.19. Utilization Plan for Edge Location Data Centre

The bidder shall provide a detailed utilization plan for the proposed edge location data Centre(s) that includes, however not limited to, the following:

1. **Proposed utilization rate:** The bidder shall provide a detailed plan that outlines the proposed utilization rate for the edge location data centre(s) over the next ten years. The plan should include revenue generation projections, projected growth rates and any expansion plans.

2. **Redundancy and resiliency:** The bidder shall provide a detailed plan that outlines the redundancy and resiliency measures that will be put in place to ensure maximum uptime and reliability for the edge location data Centre(s).

3. **Network connectivity:** The bidder shall provide a detailed plan that outlines the network connectivity options available for the edge location data Centre(s), including the number of carriers available, the type of connectivity offered, and any latency or performance guarantees.

4. **Security:** The bidder shall provide a detailed plan that outlines the security measures that will be put in place to ensure the confidentiality, integrity, and availability of the data stored in the edge location data Centre(s).

5. **Environmental considerations:** The bidder shall provide a detailed plan that outlines the environmental considerations that will be taken into account when designing and operating the edge location data Centre(s), including factors like energy efficiency and waste management.

6. **Reporting and monitoring:** The bidder shall provide a detailed plan that outlines the reporting and monitoring tools that will be put in place to track the performance and utilization of the edge location data Centre(s).

7. **Use Cases:**

   The bidder shall provide a comprehensive utilization plan that addresses all of the above requirements.

The proposals submitted by the bidder must include a proof-of-concept (POC) report showcasing the bidder's experience and expertise in the proper utilization of edge location data Centre. The report should demonstrate the bidder's ability to deploy and manage infrastructure at edge locations, including the ability to optimize network performance, ensure data security, and reduce latency.

Note : In case of edge location Data Centre, any upgradation (IT/Non IT) shall be done by the MSP.

The POC report should include the following:

1. Overview of the bidder's proposed approach to utilizing edge location data Centres.
2. Detailed description of the infrastructure to be deployed at the edge locations, including hardware, software, and networking components.
3. Performance metrics demonstrating the bidder's ability to optimize network performance, ensure data security, and reduce latency.
4. Case studies or examples showcasing the bidder's experience in deploying and managing infrastructure at edge locations.
5. A cost analysis outlining the total cost of ownership (TCO) for the proposed infrastructure.

Bidders should provide a detailed and comprehensive report that clearly demonstrates their expertise and experience in the utilization of edge location data Centres. The POC report will be a key factor in the evaluation of proposals, and bidders who do not provide a satisfactory POC report may be disqualified from consideration.

Note: As a part of effective utilization of edge location DC, the MSP must start with a minimum of 7 edge location. For further details pls refer Annexure M.

4.20. Implementation of NOC / SOC Setup

The onboarded MSP shall be responsible for setting up a fully functional NOC/ SOC at the designated STPI location. The NOC/SOC shall serve as a centralized facility for monitoring, managing, and supporting the network and security infrastructure and related services within the STPI premises.

The implemented setup shall be jointly operated by a team comprising members from both the STPI (Software Technology Parks of India) and the selected Managed Service Provider (MSP).

The NOC/SOC setup should include, but not be limited to, the following components and capabilities:

1. Robust network monitoring and management tools, including a comprehensive network management system, performance monitoring systems, and event correlation capabilities.
2. Skilled personnel with expertise in network operations and management, capable of 24/7 monitoring and responding to network incidents and issues.
3. Proactive monitoring of network devices, systems, and services, with the ability to detect and troubleshoot network faults, performance degradation, and security breaches in real-time.
4. Incident management and resolution procedures, including ticketing systems, escalation processes, and clear communication channels for reporting and resolving network incidents.
5. Documentation and reporting mechanisms to provide regular updates, performance metrics, and status reports to the STPI management, as well as participate in periodic meetings and reviews.
6. Collaboration with relevant stakeholders, including STPI management, internet service providers (ISPs), and other relevant parties, to ensure seamless network connectivity and adherence to industry best practices.

4.21. Standard Operating Procedure (SOPs)

1. The onboarded MSP shall be responsible for preparing the Standard Operating Procedures (SOP) for Data Centre (DC) operations, including the first draft of Data Centre policies for the STPI. These procedures and policies should align with all relevant government guidelines and regulations.
2. The MSP shall demonstrate a comprehensive understanding of cloud & DC operations and possess the expertise to develop SOPs and policies that encompass the necessary security, operational, and regulatory considerations for the STPI
3. The first draft of DC policies shall be developed by the MSP in collaboration with the STPI, taking into account the specific requirements and guidelines outlined by the government. The policies should address areas such as physical security, information security, data protection, access controls, incident reporting, and compliance with relevant laws and regulations
4. The MSP shall engage in close consultation and collaboration with the STPI during the development of cloud and DC policies, seeking input and approval from the STPI on key aspects to ensure alignment with the STPI's objectives and requirement.
5. The final approved SOPs, Cloud and DC policies shall be considered as binding documents, serving as the foundation for the effective and secure operation of the cloud and DC under the purview of the MSP and the STPI.

4.22. Helpdesk and Support:

The MSP will provide telephone, e-mail and web-based support to STPI officials and users of system. The STPI will provide dedicated phone numbers for Help desk, ‘This helpdesk shall be first and single point of contact for STPI officials / end users and other stakeholders. The executives in help desk will resolve any technical issues related to system. The appointed MSP will provide manpower support to the end user at ground to implement the system as asked by STPI/ End User (Departments). Required tools and infrastructures for operating helpdesk will be provided by MSP. The helpdesk will setup at STPI premises. The MSP will ensure the 100% availability of tools and required licenses to cater for 100% service capacity at the time of Go live. The MSP will provide helpdesk support through implementation of respective tools and technologies and shall provide qualified manpower for 24x7 helpdesk operations. STPI to provide space arrangements for helpdesk, NOC, and SOC. Tools to operate Helpdesk, NOC and SOC will be provided by MSP. MSP/Bidder to refer data (number of tickets and current SLA) available during the site visit.

4.23. Training

Training is an important aspect of this project, and the successful bidder will be required to undertake it in a very professional manner. The bidder will conduct a proper training needs analysis of all the staff concerned and draw up a systematic training plan in line with the overall project plan. For all these training programs the bidder must provide necessary course material and reference manuals (user/maintenance/ administration).

4.23.1. Functional Training:

This training will be focusing on the use of the monitoring system, so that the users are aware of all the operations of the internal monitoring systems and are able to implement the overall process defined by STPI for optimum use of the system. Broad training requirement defined for the purpose of calculation of effort is as follows –

I. Initial training of STPI officials on cloud infrastructure operation and management/provisioning of cloud services will be provided.

II. Routine refresh training will provide to the STPI personals on time-to-time basis
   a. Other requirements to be fulfilled by the Successful Bidder with respect to training are as follows:

III. Prepare the training material in consultation with STPI. Detailed training manuals would be prepared by MSP prior tothe start of the training.

IV. One Hard Copy & One Soft Copy of the training material will be given by the MSP to all the trainees.

V. Successful Bidder should ensure that the knowledge transfer to STPI & its staff happens effectively during thesetrainings.

VI. Professional Support/Premier Services: CSP/Cloud OEM will provide first hand support (700 hrs. per year)

VII. Physical Space, Tables, Chairs shall be provided by STPI for the training

VIII. All trainings shall be provided at DR or DC or both the locations. Any location other than the stated (Refer Section 1.2 for location) shall be decided by mutual consent between bidder and STPI.

4.24. Non-IT Infrastructure Upgradations

The Managed Service Provider (MSP) will conduct site visits to the designated STPI data centre sites in order to validate the non-IT infrastructure and assess its compatibility with the proposed solution.

If the Managed Service Provider (MSP) determines that at present or in the future, design or solution of non-IT components, such as power, cooling, or any other non-IT infrastructure elements, is not sufficient to accommodate their proposed solution, then the MSP shall bear the cost associated with such redesign or resolution.

Further, in the event that the proposed changes are approved by STPI, the MSP will be responsible for ensuring that all required modifications are implemented in compliance with industry standards and best practices. The costs incurred for the redesign or resolution shall be clearly documented by the MSP and submitted to STPI.

4.25. Expansion of Infrastructure

In the event of future expansion of the deployed solution, the MSP has the right to introduce additional technology or additional CSP technology, subject to obtaining consent from the STPI and ensuring compliance with the requirements outlined in this RFP.

The MSP will bear any additional associated costs, including procurement, implementation, training, and ongoing maintenance.

It is important to note that any future expansion must not compromise the security, performance, or stability of the existing solution. The MSP shall ensure that the integration of additional technology or

CSP does not introduce vulnerabilities, impact service levels, or violate any regulatory or contractual obligations. If multi-cloud technology is utilized upon future expansion, the governance and billing process will be consolidated and managed through a unified console.

4.26. User Acceptance Testing Go-Live and Operational Acceptance

4.26.1. Integration & Testing Phase

The MSP will provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution as a whole. The testing should be comprehensive and should be done at each stage of development and implementation.

4.26.2. Go-Live Preparedness and Go-Live

1. The MSP/CSP will prepare and agree with STPI a detailed plan for commissioning (in accordance with the implementation plan mentioned in the tender).
2. MSP/CSP will define go-live criteria and agree with STPI.
3. The MSP/CSP will submit a signed UAT (Issuance Closure Report) to ensure that all issues raised during the UAT are resolved before going live.
4. The MSP/CSP must ensure that the go-live criteria mentioned in the user acceptance tests of the project are met.
5. The launch of the application will take place in accordance with the finalized and agreed go-live plan.

Testing and Acceptance Criteria

MSP/CSP will demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. The MSP/CSP may propose further detailed Acceptance criteria which the STPI will review. Once STPI provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by STPI in mutual agreement with MSP/CSP and the revised parameters will be considered for 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 following table depicts the details for the various kinds of testing envisaged for the project.

Sr. No	Type of Testing	Responsibility	Scope of Work
1	System Testing	MSP/CSP	MSP/CSP to perform System testing
			MSP/CSP to prepare test plan and test cases and maintain it. STPI may request the MSP/CSP to share the test cases and results
			Should be performed through manual as well as automated methods
			Automation testing tools to be provided by MSP/CSP. STPI doesn't intend to own these tools
			MSP/CSP to propose the list of tools and STPI will provide the recommendation for the same
2	Integration Testing	MSP/CSP	MSP/CSP to perform Integration testing

			MSP/CSP to prepare and share with STPI the Integration test plans and test cases
			MSP/CSP to perform Integration testing as per the approved plan
			Integration testing to be performed through manual as well as automated methods
			Automation testing tools to be provided by MSP/CSP. STPI doesn't intend to own these tools
3	Performance and Load Testing	MSP/CSP/STPI/ Third Party Auditor (to monitor the performance	MSP/CSP to do performance and load testing.
			Various SLA parameters should be considered.
			Load and stress testing of the Solution to be performed on business transaction volume
			Test cases and test results to be shared with STPI.
			Performance testing to be carried out in the exact same architecture that would be set up for production.
			MSP/CSP need to use performance and load testing tool for testing. STPI doesn't intend to own these tools.
			STPI if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by STPI.
4	Security Testing (including Penetration and Vulnerability testing)	MSP/CSP/STPI / Third Party Auditor (to monitor the security testing)	The solution should demonstrate the compliance with Cyber security requirements as mentioned in the RFP including but not limited to security controls in the Cloud solutions, application, at the network layer, network, data centre(s), security monitoring system deployed by the MSP/CSP
			The solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure.
			MSP/CSP should carry out security and vulnerability testing on the developed solution. VAPT needs to be conducted for the Cloud setup including all its components established by MSP.
			Security testing to be carried out in the exact same environment/architecture that would be set up for production.
			Security test report and test cases should be shared with STPI
			Testing tools if required, to be provided by MSP/CSP. STPI doesn't intend to own these tools

			During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis.
			STPI will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSP/CSP. Cost for such auditors to be paid by STPI.
5	User Acceptance Testing of Project	STPI or STPI appointed third party auditor	STPI / STPI appointed third party auditor to perform User Acceptance Testing
			MSP/CSP to prepare User Acceptance Testing test cases
			UAT to be carried out in the exact same environment/architecture that would be set up for production
			MSP/CSP should fix bugs and issues raised during UAT and get approval on the fixes from STPI / third party auditor before production deployment
			Changes in the application as an outcome of UAT shall not be considered as Change Request. MSP/CSP must rectify the observations.

4.26.3. Final Acceptance Testing

The final acceptance shall cover 100% of the Project, after successful testing by the STPI or its PMU; a Final Acceptance TestCertificate (FAT) shall be issued by the STPI.

Prerequisite for Carrying out FAT activity:

I. Detailed test plan shall be developed by the MSP/CSP and approved by STPI. This shall be submitted by MSP/CSP before FAT activity to be carried out.
II. All documentation related to the project and relevant acceptance test document (including IT Components, non-IT Components etc.) should be completed & submitted before the final acceptance test to the STPI.
III. The training requirements as mentioned should be completed before the final acceptance test.
IV. Successful hosting of Application, NMS, and MIS Software.
V. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the project supplied components.

The FAT shall include the following:

I. All hardware and software items must be installed at respective sites as per the specification.
II. Availability of all the defined cloud services and solutions shall be verified.
III. The MSP/CSP will be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
IV. The MSP/CSP will arrange the test equipment required for performance verification and will also providedocumented test results.
V. The MSP/CSP will be responsible for the security audit of established system to be carried out by a certified thirdparty as agreed by STPI.

Any delay by the MSP/CSP in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of MSP/CSP shall be considered appropriately and as per mutual agreement between STPI and MSP/CSP. In the event the MSP/CSP is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the MSP and STPI may mutually agree to redefine the Network so the MSP/CSP can complete installation and conduct the Final Acceptance Test within the specified time.

4.27. RACI Matrix

The identified stakeholders for this project include the following:

a) STPI
b) MSP (Managed Service Provider)
c) CSP (Cloud Service Provider)
d) End Users Customers (Departments/ Users, using services)

The table below provides a comprehensive breakdown of the roles and responsibilities assigned to the stakeholders that have been identified.

RACI (Responsible, Accountable, Consulted, and Informed)

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
1	**Planning and Design of IT Infrastructure Resources as per STPI Current and Future Requirements**			
1.1	Site Survey of DC and DR along with different edge locations data centre	I	R, A	
1.2	Sizing of revised Electrical and Mechanical load based on own requirement and provision of additional UPS power if required.	I	R, A	
1.3	Provisioning of Electricity meter for Hybrid Cloud, 1 rack & GCC, 10 racks space allocated at each DC	R, A	I	
1.4	Entering O&M Contract with all OEMs of IT Infra and upkeep of all IT equipment as per SLA required in RFP SoW	I	R, A	
1.5	Upgrade of any IT Infra (Server, storage, network devices etc.), if required	I	R, A	
2	**Planning and Design of Infrastructure Resources as per STPI Current and Future Requirements**			
2.1	Planning of placement of IT infrastructure resources	I	R, A	
2.2	Design of new DC and DR infrastructure to provide required performance	I	R, A	

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
2.3	Availability of required resources at DC- DR and edge location that meets the STPI growth requirements	I	R, A	
2.4	Enable scale-in and scale-out of resources as per requirement	I, C	R, A	
2.5	Manage affinity rule of instance for better resilience and performance	I	R, A	
2.6	Mitigation of any single point of failure of IT and Non-IT Infrastructure (only for edge location).	I	R, A	
2.7	DC and DR Cloud service provisioning and availability (as per SOW/Annexures)	I	R, A	
2.8	Procurement and installation of all network links as required for the project	C, I	R, A	
2.9	Monitoring of all network links as required for the project.	I	R, A	
2.10	NOC and SOC connectivity to DC and DR.	I	R, A	
2.11	Procurement of Insurance for all the Non -IT (only for edge location) and assets deployed at DC and DR at edge locations for STPI	I	R, A	
3	**Infrastructure Administration & Management including Cloud services**			
3.1	End to end Management of IT Infrastructure resources	I, C	R, A	
3.2	Managing of IT infrastructure provisioning and decommissioning	I	R, A	
3.3	Managing break/fix of Infrastructure hardware	I	R, A	
3.4	Managing availability of IT Infrastructure instances	I	R, A	
3.5	Active monitoring and performance management of IT infrastructure resources	I	R, A	
3.6	Template management for custom OS images and required sizing	I	R, A	
4	**Hybrid Cloud Management**			
4.1	Cloud Solution installation (OS Installation, Middleware Installation, On-prem cloud solution installation (including all modules as per Scope)	I	R, A	
4.2	Cloud Solution patching and integration	I	R, A	

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
4.3	OS vulnerability management	I	R, A	
4.4	Cloud Solution upgrade related activities	I	R, A	
4.5	Firmware upgrade of all hardware infrastructure	I	R, A	
4.6	Update of Hypervisors	I	R, A	
4.7	Update of Storage, Network, Security Software's etc.	I	R, A	
4.8	Update of NOC, SOC, SLA Mgmt., and Reporting, KPI Mgmt. etc.	I	R, A	
4.9	Billing Management (Tool) on behalf of STPI	I	R, A	
5	**Managed Backup Services**			
5.1	Configuration of backup of databases and application data	I	R, A	
5.2	Installation of backup agents in all required machines (If required)	I	R, A	
5.3	Setup of different types of backups as per requirement (Full and Incremental)	I	R, A	
5.4	Snapshot backups of VMs	I	R, A	
5.5	Manage the retention period of daily, weekly, and monthly backups	I	R, A	
5.6	Regular monitoring of backup success and failures	I	R, A	
5.7	Periodic backup and restoration testing	I	R, A	
5.8	Perform restoration and help in database/application recovery operations as needed	I	R, A, C	
6	**Managed Disaster Recovery Services**			
6.1	Planning and setup of DR site and resources (Including DRM tool)	I	R, A	
6.2	Setup of DR resources and finalize replication methodology	C, I	R, A	
6.3	Manage and meet defined RPO and RTO for all applications	C, I	R, A	
6.4	Manage and meet defined RTO for all services	I	R, A	

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
6.5	Replication tool and services	C	I	
6.6	Perform DR Drill	I	R, A	
7	**API / Other solution Integration**			
7.1	Integration of various Solutions and API as per STPI program requirement	I	R, A	
8	**Asset and Inventory Management**			
8.1	CMDB management	I	R, A	
8.2	Hardware & its OS and firmware Management i.e., Network, computer, storage, and backup	I	R, A	
9	**Managed Network Services**			
9.1	Setup and configuration of network and connectivity services	I	R, A	
9.2	Administration and operation of an end-to-end STPI network including WAN, LAN for Data Centre locations	I	R, A	
9.3	Manage availability and performance of network bandwidth	I	R, A	
9.4	Manage STPI Domain name	I	R, A	
9.5	Manage DNS, DHCP, Domain controller, LDAP services	I	R, A	
9.6	Monitor and fix network failures, disruption in network	I	R, A	
9.7	Plan for network upgrades, removal of bottlenecks, capacity constraints in bandwidth	I	R, A	
9.8	Monitoring and reporting of network performance and usages	I	R, A	
10	**Managed Security Firewall and Security Services**			
10.1	End to end managed security services including	I	R, A	
10.2	Network Security Devices	I	R, A	
10.3	Web and Email Security Devices (Web Gateway and Email Gateway)	I	R, A	
10.4	DLP appliance	I	R, A	

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
10.5	IAM, PIM, SSO, MFA and Active Directory services	I	R, A	
10.6	HIPS and Antivirus Tools, Drives and file encryption	I	R, A	
10.7	Security Management Tools	I	R, A	
10.8	Encryption devices (PKI, HSM)	I	R, A	
10.9	Configuration management, administration, maintenance services for all components listed	I	R, A	
10.1	Implementation and review of security rules and policies	I	R, A	
10.11	Identity and access management of all user roles and groups and access review	I	R, A	
10.12	Security incident management and reporting	I	R, A	
10.13	Vulnerability assessment, reporting and mitigation	I	R, A	
11	**Monitoring Services**			
11.1	ICMP/Ping monitoring of all IT Infrastructure resources and Object storage	I	R, A	I
11.2	Monitoring of IT Infrastructure resources utilization (i.e., Compute, Storage, network etc.)	I	R, A	I
11.3	OS Metrics Monitoring, logging, and event Management	I	R, A	I
11.4	Monitoring of open-source services configured and reporting	I	R, A	I
11.5	Network Performance Monitoring	I	R, A	I
11.6	Provide a console to visualize the KPIs, metrics and logs	I	R, A	I
11.7	Creating the Informational/Warning/Critical notifications for defined threshold values	I	R, A	I
11.8	Comprehensive proactive monitoring and reporting of OS/Services/Warning/Critical alerts/events	I	R, A	I
12	**Service Level Agreements**			
12.1	Availability of critical services	I	R, A	I
12.2	Uptime of IT Infrastructure resources	I	R, A	I
12.3	Infrastructure resources performance SLA	I	R, A	I
12.4	Incident and service request SLA	I	R, A	I
12.5	24*7 Support services SLA	I	R, A	I

#	RACI Matrix	STPI	MSP/CSP	End User / Customers
13	**Support Services**			
13.1	24 x 7 Support for NOC and SOC	I	R, A	I
13.2	Define priority of issues and service request (i.e., Severity 1,2 and 3, etc.)	I	R, A	I
13.3	Incident management and reporting	I	R, A	I
13.4	Provide root cause analysis for critical issues related to infrastructure	I	R, A	I
13.5	Remote NOC and SOC as well as onsite teams to provided end to end support on managed services	I	R, A	I

#	Activity to be Performed	STPI	MSP	END User
1	**Network Support**			
a	Manage, operate, and support the network and communication infrastructure	I	R, A	
b	Ensure connectivity between all endpoints on the DC network scope	I	R, A	
c	Monitor network for problems, performance, and capacity	I	R, A	
d	Install, upgrade, and performance manage infrastructure and software	I	R, A	
e	Plan, operate, administer, manage, and document the network and other infrastructure	I	R, A	
f	Perform provisioning, staging, configuration, installation, site surveys and upgrading of network systems and equipment	I	R, A	
g	Prepare designs for network modifications or upgrades to meet changes in demand including those for capacity, performance and modifications to services or technology	I	R, A	
h	Perform root-cause analysis on network-related problems and implement effective solutions to mitigate their effect and prevent their recurrence.	I	R, A	
2	**Server Operations and Support**			
a	Manage, provision, and provide operational support for all physical and virtual servers and associated storage and other infrastructure	I	R, A	

#	Activity to be Performed	STPI	MSP	END User
b	Continuously monitor performance of network traffic and take appropriate effective remedial action when alerts are activated	I	R, A	
c	Continuously monitor infrastructure hardware and take appropriate effective remedial action when alerts are activated	I	R, A	
d	Continuously monitor infrastructure software and take appropriate effective remedial action when alerts are activated	I	R, A	
e	Continuously monitor application availability and performance and take appropriate effective remedial action when alerts are activated	I	C	
f	Perform root-cause analysis on system hardware and software related problems and implement or recommend effective solutions to prevent their recurrence as appropriate	C, I	R, A	
g	Implement special operating instructions and change request authorizations	R, A	I, C	
h	Perform and report on scheduled out-of-business-hours operating system and infrastructure software maintenance including system patching every month	I	R, A	
i	Monitor all scheduled activities including data backup and detect and rectify any failure within agreed timeframes	I	R, A	
j	Perform server start-ups and shutdowns and execute utilities in accordance with application guidelines where these guidelines are applicable	I	R, A	
k	Configure, manage, and support all server equipment, operating systems, utilities, and other infrastructure software	I	R, A	
l	Maintain inventory of server equipment and software, including locations, configuration, and release levels	I	R, A	
m	Provision new server equipment and software, including, staging, configuring, processing end user requests and installation	I	R, A	
n	Manage and monitor server and disk storage performance to ensure sufficient capacity and efficient utilization	I	R, A	
o	Develop forecasts of server and disk storage growth and other changes in response to projected business needs	I	R, A	

#	Activity to be Performed	STPI	MSP	END User
p	Manage and maintain disaster recovery systems and infrastructure to ensure that they will deliver all services to appropriate levels of availability and functionality if they need to be used as STPI's operational production environment	I	R, A	
q	Perform disaster recovery testing using the DRP on a six- monthly basis and as requested	I	R, A	
r	Provide a written report on the results and outcomes of DR testing and recommend changes to the DRP and DR systems and infrastructure to address any shortcomings	I	R, A	
s	Execute the DRP when requested to by STPI’s IT Management in the event of an actual loss of availability of its production systems and infrastructure (i.e., in a “disaster” event).	I	R, A	
3	**Capacity Planning**			
a	Manage and maintain systems and infrastructure capacity as required to ensure that the services are provided to the required levels of availability	I	R, A	
b	Add, remove, or reallocate capacity as required and as authorized	I	R, A	
c	Forecast capacity requirements as part of STPI’s normal business planning cycle	I	R, A	
d	Maintain inventory of Capacity utilization and estimates	I	R, A	
e	Data protection and encryption	I	R, A	
4	**Security Services**			
a	Administer security services and facilities ensuring that they are always current	I	R, A	
b	Reset passwords according to approved procedures	I	R, A	
c	Identify and respond to security breaches within agreed timeframes	I	R, A	
d	Monitor for security breaches and implement corrective actions to prevent further breaches. Provide a written report regarding the breach including mitigation strategies implemented within agreed timeframes	I	R, A	
e	Recover, to the extent possible, information that is lost or damaged as a result of a security breach	I	R, A	
f	Perform security audits, including periodic audit self- assessments as defined by STPI	I	R, A	
g	Take all action necessary to prevent interception of data that is transmitted over the data network under its control	I	R, A	

#	Activity to be Performed	STPI	MSP	END User
h	Provide direct, indirect, immediate, and unimpeded access to all information and assets for investigations, audits, and compliance reviews	I	R, A	
i	Evaluate, develop, implement, and maintain tools and processes to allow secure access to the internal network by end-users at remote locations	I	R, A	
j	Contribute to the development and maintenance of STPIS's IT related policies and procedures including IT Security Policy, Security Plan, Security Calendar etc.	R, A	C, I	
k	Perform scheduled internal and external system vulnerability scanning every 6 months	I	R, A	
l	Perform scheduled out-of-business-hours operating system and infrastructure software patching is accordance with the Patch Management and System Maintenance Process	I	R, A	
m	Perform directory administration functions, including development, installation and maintenance of directories, directory structures and naming conventions; purging records, files, and old end user accounts; and restoration of deleted files upon request	I	R, A	
n	Audit and review on account access rights and privileges every 3 months or as requested	I	R, A	
o	Third-party assessment of complete security infrastructure, rules, policies, compliance to regulations and governance.	R, A	C, I	
p	Prove all inbound and outbound traffic logs of On-prem and Cloud Infra to STPI team	I	R, A	

4.28. Manpower Requirement

With a project of this size and complexity, it is essential that MSP deploy the best professionals available to ensure the successful execution of Project, MSP will include in its proposal the name and detailed CV of the minimum on-site resource working full time on the project.

4.28.1. Deployment of Resources

The MSP must have a sufficient number of qualified technical personnel capable of supporting the operation of the project in the manner required by STPI and meeting the SLA and scope of work. The MSP must deploy the required labour based on the offer to meet the SLA and scope of work negotiated with STPI.

The STPI will provision space resources as at its various location. For the key personnel working out at STPI location, the STPI will provide them with basic office infrastructure like seating space, internet connection. The MSP team is expected to bring their own laptops and any required tools. MSP should plan for the regional deployment of its team. Also, all travel costs of its resources for project related work including meetings with customers etc. shall be borne by MSP.

4.28.2. Key Resources of the MSP

Bidders share resource deployment plans that will be evaluated by STPI as part of the technical bid. The planned size of resources may be shared among bidders and STPI reserves the right to accept/reject and finalize the mutually agreed resource deployment plan. The project team will include at least expertise and experience in the following disciplines.

4.28.3. Tentative list of resources for managing own Infrastructure:

S.no.	Role
1	Engagement Director
2	Project/Program Manager
3	Network Administrator
4	System Administrator
5	Backup Administrator
6	Storage Administrator
7	MySQL database administrator
8	PostgresDB Administrator
9	MS-SQL database administrator
10	NOC – L1
11	NOC – L2
12	NOC – L3
13	Cyber Security Engineer
14	Cloud Operations Engineer
15	Cloud Services Manager
16	Cloud Administrator
17	BCP/DR Specialist
18	IT Service Desk L1 Engineers
19	IT Service Desk Manager Engineers – end-user device support, LAN management, etc.

4.28.4. Skills needed from Remote NOC and SOC for remote infrastructure management

S. No.	Role
1	SOC Administrator (L3)
2	SOC Analysts (L1)
3	ITSM Tool Expert (L2)
4	System Administrator (L2)
5	Voice & Video Administrator (L2)
6	Server Architect (L2)
7	EMS Administrator (L2)
8	Network Architect (L2)
9	Storage and Backup Administrator (L2)
10	Network Administrator (L2)
11	Network Security Expert (L2)
12	PKI and HSM Expert (L2)
13	Identity Access Management and SSO Expert (L2)
14	PIM, PAM, and MFA Expert (L2)
15	Database Activity Monitoring Expert (L2)
16	Secure Configuration Management and File Integrity Monitoring Expert (L2)
17	DLP Expert (L2)
18	Endpoint Security Expert (L2)
19	SIEM Expert (L2)
20	Network User and Events Behaviour Analytics Expert (L2)
21	Cloud Migration Solution Architect- Minimum of 5 years of relevant experience
22	Cloud Migration DevOps Engineer- Minimum 5 years of relevant experience
23	Cloud Migration Systems Admin Minimum 5 years of relevant experience
24	Project Management- Application Expert

4.28.5. Resource Responsibilities and Minimum Resource Qualifications

The following table specifies the minimum qualification required for Key Positions identified for this project.

S. No.	Position	Key Responsibilities	Minimum Qualifications
1	Program Manager	• Overall program governance during implementation of the project • Stakeholder coordination and management • Single point of contact during implementation of the project • Overall risk management and responsible for resolution of critical project issues • Monitoring overall project progress • Overall delivery and operations management • Team management and coordination with various team members to resolve • any conflicts and issues during implementation and O&M phases	• Total Experience: should possess at least 18 years of experience in IT domain • Should have more than 10 years of experience of handling such large projects as a project/program manager • Should possess Project Management certifications like PMP or Prince2 • Should have managed projects preferably in the India • Should have led at least one such project end to end i.e., from development to deployment to O&M • Should have managed at least three projects related to private cloud setup • Languages known – English • Previous experience of handling large IT projects in Public Sector would be an added advantage

S. No.	Position	Key Responsibilities	Minimum Qualifications
2	IT Infrastructure Lead	• Responsible for study of current IT infrastructure and prepare To-Be design of IT infrastructure • Monitoring progress of IT infrastructure setup • Coordination with various IT infrastructure administrators for implementation and commissioning of IT infrastructure • Coordinate with AP for implementing any application specific requirements • Technical expertise on overall IT infrastructure components as required • Single point of contact for IT infrastructure setup • Provide L2 support onsite for any issues on IT • Infrastructure • Coordinate with NOC • Team for timely resolution of issues • Coordinate with AP support team for timely resolution of issues. • Coordinate with cyber security lead for timely resolution of issues	• Total Experience: The resource should have a minimum of 12 years' experience in IT Infrastructure domain with at least 7 years' experience in managing large IT Projects • The resource should have worked in at least three project of private cloud deployment and management

S. No.	Position	Key Responsibilities	Minimum Qualifications
3	Cyber Security Engineer	• Responsible for study of current cyber security infrastructure and prepare To-Be design of Cyber Security setup • Monitoring progress of IT infrastructure setup • Coordination with various cyber security domain experts for implementation and commissioning of cyber security setup • Coordinate with AP for implementing any application specific cyber security requirements • Technical expertise on overall cyber security components as required • Single point of contact for Cyber Security setup • Provide L2 support onsite for any issues on Cyber Security Setup • Coordinate with SOC team for timely resolution of issues • Coordinate with AP support team for timely resolution of issues • Coordinate with IT infrastructure lead for timely resolution of issues. • Coordinate with remote SOC team to check status of daily activities, incident management and resolution • Assist remote SOC team in building and finetuning use cases as well as fine-tuning / configuration management of various security solutions deployed in STPI.	• Should have experience of more than 10 years in implementation and managing cyber security projects • Should have handled cyber security implementations in at least 2 largescale projects • Should have worked in at least three projects of private cloud cyber security deployment and management. • Should be CISSP certified
4	IT Service Desk Manager	• Ensures support staff has adequate skill levels • Execution of the Incident Management process • Is responsible within their specific domain to manage the Incident Management process • Request and review metrics reports • Provides management information on IT service quality and Customer satisfaction • Manage support staff performance of the Incident Management process, creating and executing action plans when necessary to ensure continuous improvement • Own management review	Experience: He/she should have a minimum of 5 years experience as LAN/System Administrator or in System Administration Support.

S. No.	Position	Key Responsibilities	Minimum Qualifications
		process of Incidents that are not resolved through the standard Incident Management process • Know how to engage next level of management • Detection of possible Problems and the assignment of them to the Problem Management team for them to raise problem records • Providing guidance on moving an Incident from Active to Technical Review to Management review level • Monitors service delivered by the team for all Customers being served • Executing the Incident Management process • Assisting the support engineers through the Incident Management process within their domain • Provides service delivery metrics to Service Centric Performance Management team. • Identifying Process improvement • Re-evaluating workload between support levels • Review effectiveness and efficiency of the Incident Management process • Establish procedures for Incident Management process • Ensure Incident Management process and tools integrate with other ITSM processes • Communicates the process roles and responsibilities • Provides issue resolution support and service request fulfilment to end-users for issues and service requests that can be resolved remotely	
5	IT Service Desk L1 Engineers	• One team member shall man the service desk to handle calls from end-users. • Provide onsite support for resolution of issues pertaining to endpoints, LAN, printers, etc. • Coordinate with vendors of endpoints, printers for any warranty/AMC related issues	• Experience: He/she should have a minimum of 5 years experience of managing Data Centre IT and Security Systems(Servers, HCI, storage network, security, etc.).

S. No.	Position	Key Responsibilities	Minimum Qualifications
6	IT Engineers (L1)	• Provide basic troubleshooting support for IT infrastructure and Cyber Security components at the Data Centre • Coordinate with IT infrastructure and Cyber Security lead for resolution of issues • Carry out day-to-day administration activities covering all IT infrastructure and Cyber Security components and processes including all databases.	• Experience: He/she should have a minimum of 5 years' experience of managing Data Centre IT and Security Systems (Servers, HCI, storage, network, security, etc.).
7	Cloud Migration Solution Architect	• Act as an overall architect for Cloud Migration Solution Design and delivery and client facing activities • Design architectural standards for cloud services, Design and implement global management tools and framework for governance and cost controls • Architect and develop tools and solutions to integrate, automate, and orchestrate cloud operational needs • Create implementation guidelines and reusable design templates wherever possible • Establish engineering and automation objectives • Consult with internal IT customers on net new and cloud migration initiatives • Provide third-level support and provide root cause analysis of issues • Maintain security standards in cloud per Security guideline and benchmarks • Assist in capacity planning	• Experience: 5 years of relevant experience
8	Cloud Migration DevOps Engineer	• Application migration to the multi-cloud in project delivery cycle with hands on experience migrating customers/projects to the cloud. • This role includes ownership of technical commercial, and service elements related cloud migration project engagements along with building IaaS/PaaS infrastructure landing zones • Handle cloud migration technologies and Cost analysis. • Hybrid cloud solutions and experience integrating public cloud into tradition hosting/delivery models • Implement cloud migration	• Experience: 5 years of relevant experience

S. No.	Position	Key Responsibilities	Minimum Qualifications
		techniques and workflows (on premise to Cloud Platforms)	
9	Cloud Migration Systems Admin	• Application migration to the multi-cloud in the project delivery cycle with hands on experience migrating customers/ projects to the cloud. • Work closely with clients, partners, and other business units to ensure consulting engagements are successful. • Take ownership of technical, commercial, and service elements related to cloud migration project engagements along with building IaaS/PaaS infrastructure landing zones. • Experience with cloud migration technologies of loud and Cost analysis. • Strong Experience on hybrid cloud solutions and experience of integrating public cloud into tradition hosting/delivery models • Implement cloud migration techniques and workflows (on premise to Cloud Platforms)	• Experience: 5 years of relevant experience
10		• Develop the project schedule and plan to ensure timely completion of the project. Obtain management and client agreement with the project plan and timeline, and advise of any obstacles or resource needs that may affect completion of the project as planned • Assemble the project team, identify competencies, and assign resources to development tasks appropriate to each individual's knowledge, skill, and abilities • Apply project management tools and tracking systems to manage all aspects of project progress • Utilize project resources and serve as an individual contributor to develop programming code or software modifications using appropriate languages and tools to optimize resources and meet functional user requirements • Utilize project resources and serve as an individual contributor to analyse user system and application needs, determine, and evaluate potential solutions,	• Experience: 5 years of relevant experience

S. No.	Position	Key Responsibilities	Minimum Qualifications
		develop system specifications and requirements, and design application programs to meet the requirements • Utilize project resources and serve as an individual contributor to design integrated solutions which may include applications, databases, networks, and related systems • Utilize project resources and serve as an individual contributor to structure, implement, and maintain database systems. Establish policies, standards, and procedures to ensure useful and readily accessible data	
11	System Administrator	• Managing security, compliance & accreditation including internal and external regulations and policies • Perform server maintenance in production and non-production environments • Supporting the service / Help Desk with day-to-day end-user assistance, incident troubleshooting and resolution, and physical IS asset re-location • Supporting catalogue requests including accepting, approving, and fulfilling provisioning requests • Managing the maintenance of server's operating systems	• Experience: 5 years of relevant experience Certification: Linus Administration
12	Network Administrator	• Experience in daily network operational tasks that would include configurations, communication performance, in a secure, reliable, and highly availability environment • Experience in operation and support of Application Centric Infrastructure (ACI) • Familiarity with and demonstrated understanding of enterprise's business and technical architecture. • Hands-on technical knowledge of network systems, protocols, and standards such as ethernet, Wi Fi, LAN, WAN, STP, VPC, VxLAN etc.,) • Minimum of 3 years' experience working in a switched and routed environment (OSPF, BGP, MPLS, MPBGP, VPN etc.,) • Operation and support of	• Experience: 3-5 years of relevant experience Certification: Cisco/ Juniper Professional Certification in Data Centre Networking in mandatory.

S. No.	Position	Key Responsibilities	Minimum Qualifications
		application load balancer: F5 (LTM & GTM).	
13	NOC Engineer L1	• Performing regular checks on network hardware and software. • Responding to network alerts and hardware malfunctions. • Diagnosing and troubleshooting network errors. • Tracking and documenting network issues and compiling incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols • Performing regular checks on network hardware and software. • Responding to network alerts and hardware malfunctions. • Diagnosing and troubleshooting network errors. • Tracking and documenting network issues and compiling incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols.	• Experience: 2 years of relevant experience Certification: Any associate network certification., Windows and Linux administration
14	NOC Engineer L2	• Responding to network alerts and hardware malfunctions. • Diagnosing and troubleshooting network errors. • Tracking and documenting network issues and compiling incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols • Performing regular checks on network hardware and software. • Responding to network alerts and hardware malfunctions. • Diagnosing and troubleshooting network errors. • Tracking and documenting network issues and compiling	Certification: Any associate network certification., Windows and Linux administration

S. No.	Position	Key Responsibilities	Minimum Qualifications
		incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols.	
15	NOC Engineer L3	• Troubleshooting Network errors. • Tracking and documenting network issues and compiling incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols • Performing regular checks on network hardware and software. • Responding to network alerts and hardware malfunctions. • Diagnosing and troubleshooting network errors. • Tracking and documenting network issues and compiling incident reports. • Responding to user requests and providing network training. • Managing system backups and network security protocols.	• Experience: 7 years of relevant experience Certification: Any associate network certification., Windows and Linux administration
16	Cloud Services Manager	• Ability to provide a planned migration to cloud services in line with the Infrastructure as a Service strategic direction • Ability to undertake tasks in a dynamic environment including meeting deadlines, demonstrating commitment to customer service, working with limited supervision, and adhering to workplace standards, procedures, and agreements • Understand and leverage network, server, and monitoring system APIs (Cisco, F5, HP) to automate provisioning • Plan, coordinate and manage on-boarding of new internal customers, including activities the internal customer and operations team need to take to prepare for the operations transition	• Total Experience: The resource should have a minimum of 12 years' experience in IT Infrastructure domain with at least 7 years' experience in managing large IT Projects. Certification: Architecture level cloud certifications from proposed CSP is mandatory.

S. No.	Position	Key Responsibilities	Minimum Qualifications
		• In depth knowledge on Windows/Linux OS, Networking and Internet Protocols, DevOps and Containerization, Virtualization, Cloud Service Providers, Security and Recovery, Web Services and API. • The resource should have worked in at least three project of private cloud deployment and management.	
17	Cloud Operations Engineer	• Understanding the needs for new initiatives to build scalable, distributed, and high-performance computing cloud-based platform solutions on relevant cloud platforms • Deploying and debugging Cloud initiatives as needed in accordance with best practices throughout the development lifecycle • Performing operating system and software application installation, patching, and upgrades. • Good knowledge on Windows/Linux OS, Networking and Internet Protocols, DevOps and Containerization, Virtualization, Cloud Service Providers, Security and Recovery, Web Services and API. • Educating teams on the implementation of new cloud-based initiatives, providing associated training as required • Troubleshooting and resolving issues reported by monitoring systems and submitted through the ticketing system of fully documented issues, actions taken, and steps for resolution • Performing other tasks as defined, planned, and approved by leadership • The resource should have worked in at least one project of private cloud deployment and management.	• Total Experience: The resource should have a minimum of 3 – 5 years' experience in IT Infrastructure domain with at least 7 years' experience in managing large IT Projects. Certification: Any Associate level cloud certifications from proposed CSP is mandatory.

S. No.	Position	Key Responsibilities	Minimum Qualifications
18	Backup Administrator	• Experience in monitoring the state of backup/recovery resources including the availability of allocated backup storage space, replication to offsite • Experience in managing the inventory of offsite storage of backup media and ensure that backup media handling conforms to established procedures • Familiarity with and demonstrated understanding of enterprise's business and technical architecture. • Experience in archival processes, strategies, and tools • Experience in enterprise storage management systems • Experience working on large enterprise backup & recovery initiatives • Extensive experience in scheduling backup operations, including job creation, scheduling, and backup completion status monitoring across all platforms	• Experience: Minimum 3-5 years' experience. Certification: Storage and Backup Technology Certification, Windows Server Administration. Red Hat Certified System Administrator
19	Storage Administrator	• Knowledge of storage hardware architectures • Familiarity with high-level programming languages • Experience working in a distributed file systems environment • Stays up to date on new technologies to ensure they offer the latest solutions to their clients • Experience adding and removing disks, disk group management, logical unit numbers (LUN) management and provisioning. • Experience planning, monitoring, repairing, and reporting on storage resources. • Experience with infrastructure capacity planning. • Demonstrated understanding of enterprise's business and technical architecture. • Experience providing general IS user support. • Mentor and guide Storage Administrators in carrying out related activities. Coordinate and delegate tasks as required. • Provide guidance and coaching to Storage Administrators	• Experience: Minimum 5 years' experience Certification: Storage Technology Certification, Windows Server Administration, Red Hat Certified System Administrator

S. No.	Position	Key Responsibilities	Minimum Qualifications
		regarding deliverables and related processes. • Experience on large storage management initiatives • Experienced installing and configuring SAN storage controllers.	
20	Database Administrator (MySQL/ PostgresDB/ MS-SQL/MongoDB)	• Experience in daily database operational tasks that would include configurations, performance, backup, recovery, disaster recovery scenarios and manage data in a secure, reliable, and highly available system environment • Knowledge of database storage infrastructure • Experience in planning, monitoring, repairing, reporting and other day-to-day tasks associated with maintaining database resources in an optimal fashion. • Experience in Infrastructure capacity planning • Familiarity with and demonstrated understanding of enterprise's business and technical architecture.	• Total Experience: The resource should have a minimum of 5 years' experience in IT Infrastructure domain with at least 7 years' experience in managing large IT Projects. Certification: Any Associate level cloud certifications from the proposed CSP is mandatory
21	Cloud Administrator	• Configuring the cloud management service • Managing the cloud management service. • Integrate cloud-based systems into the existing environment. • Resolve operational issues. • Change requests for cloud management service upgrades must be approved or denied. • Key metrics for cloud resources should be monitored. • Load balancing. • New cloud computing	• Total Experience: The resource should have a minimum of 3 – 5 years' experience in IT Infrastructure domain Certification: Any Associate level cloud certifications from the proposed CSP is mandatory

S. No.	Position	Key Responsibilities	Minimum Qualifications
		technologies should be evaluated and implemented. • Examine summary data from cloud resource deployments.	
22	BCP DR Specialist	• Ownership and management of business continuity and disaster recovery for complete cloud platform to DR site or public cloud. • Responsible for ensuring development of recovery plans by each of the recovery teams • Perform Business Impact Assessment (BIA) • Ensure proper maintenance of the plan through regular reviews with teams • Schedule, coordinate and conduct planned tests, as required, and Perform risk assessment • Develop, coordinate, and assess recovery requirements and contingency plans • Develop contingency plans to deal with emergencies • Analyse impact on, and risk to, essential business functions or information systems to identify acceptable recovery time periods and resource requirements • Assess risks to business operations • Conduct or oversee contingency plan integration and operation • Create or administer training and awareness presentations or materials • Contingency Planning – Identify potential business interruptions, develop safeguards against these interruptions, and implement recovery procedures in the event of a business interruption. Provide • Documentation and training on contingency planning concepts and procedures.	• Experience: Over 8 years of IT experience and 7 years' management experience in Business Continuity and Disaster Recovery Certifications: Certifications in Project Management would be beneficial to performing this role, ITIL is required, BCI is desirable.

S. No.	Position	Key Responsibilities	Minimum Qualifications
		• Excellent exposure to operations, production, and technology environments	
23	Engagement Director	• Creating and maintaining relationships with different government departments and STPI • Developing strategies to increase brand awareness and increase workload from different tenants to On-premises cloud. • Assisting customers in providing more value from the services. • Analyse customers' needs and suggest additional features/services to meet their requirements • Track account metrics. • Good technical and product knowledge. • Excellent communication and interpersonal skills • Good critical thinking and problem-solving skills.	• Experience: Over 15 years of IT experience and 10 years' management experience in Business Continuity and Disaster Recovery

Note:

a. Onsite IT Service Desk team shall be bilingual (English and Hindi)

b. Onsite resources of the project as proposed in the technical proposal should not be changed without STPI's approval.

c. The MSP should provide the Resources Availability & Replacement plan in case resources deployed for the project in cases of leaves, medical issues, death, resignation, etc.

d. In a case any onsite resource is on leave for more than 2 working days in a month, the MSP shall arrange for a suitable replacement resource onsite for the same period.

e. In case of resignation of an onsite resource deployed in this project, the MSP shall ensure that the replacement resource is available onsite for at least 30 days working in parallel with the resource that has resigned.

f. Onsite resources deployed shall have proper tools for managing the infrastructure.

g. STPI reserves the right to interview the key resources prior to their deployment

h. The offsite L1, L2 and L3 resources shall have at least 3, 5, and 8 years of experience respectively in their respective technology/tool/functional areas in-line with industry standards and STPI reserves the right to seek the details of such resources and can verify the same on need basis and MSP shall comply with these requirements.

i. The MSP should have SOC analyst resources who are certified on security monitoring from SANS.

j. The onsite L1 IT engineers shall be included as part of any new infrastructure deployment activities.

k. The onsite L1 IT engineers shall be deployed having multiple skillsets covering servers, HCI, storage, network, security, and backup.

l. While the onsite L1 IT engineers are expected to be deployed on 24x7 basis, STPI may change the deployment of such resources in the future in-line with overall service support requirements. MSP will conduct background verification of all resources deployed in the project. Criteria for BG verification can be mutually agreed in discussion with STPI

4.29. Timelines

#	Component	Timeline (in month)
1	Go- Live of mutually decided first hybrid setup location	T+3 months
2	Setup and release of Hybrid Cloud services at second data centre location	T+4 months
3	Setup and release of Hybrid Cloud services at other three Data Centre locations	T+5 months
4	Setup of Infrastructure and release of services at STPI edge locations	T+5 Months
5	Setup of Government Community Cloud (GCC) at first GCC location and release the services	T+6 months
6	Setup of Government Community Cloud (GCC) at second GCC location and release the services	T+7 months
7	Setup of DC-DR, after successful DR drill	T+7 months
8	Final signoff a. Provisioning of Advanced and Specialized services for multisite deployment b. Launching of Hybrid Cloud Provisioning and Management Layer to integrate all sites, self-service portal and billing mechanism	T+9 months

#	Component	Timeline (in month)
	c. Testing and user acceptance of overall Cloud platform	

Where - T is the date of signing of contract with the MSP

- MSP shall apply for the MeitY Empanelment for the cloud services within 3 months from the start of that respective cloud setup of that particular location.
- The MSP shall manage the Hybrid Cloud and GCC setup for next 10 years post commissioning (approx. 123 months)
- The data Centre locations stated above are tentative and may change as per the requirements by STPI before final implementation.

Section V: Formats for Bid Submission

Annexure A: Bid Covering Letter

[To be submitted on the letterhead of the bidder]

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Submission of bid in response to the RFP for "Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model".

Dear Sir,

We have examined the conditions of RFP, Scope of Work and other technical specifications. We, the undersigned offer ourselves as a competent IT agency to take up the project named "Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model" in accordance with the Terms & Conditions specified in the RFP for the offer mentioned in our Commercial Proposal.

We undertake, if our Proposal is accepted to commence work within 15 (fifteen) days from the date of issuance of the relevant Work Order. If our Proposal is accepted, we will furnish the Contract Performance Bank Guarantee as specified in the RFP document.

We agree to abide by this Proposal for a period of 180 days from the date fixed for opening of the Technical Proposals and it shall remain binding upon us and may be accepted at any time before the expiration of that period. Until the Work Order or Contract is prepared and executed, this Proposal together with your written acceptance thereof in your notification of award shall constitute a binding contract between us. We understand that you are not bound to accept the lowest or any proposal you may receive.

Dated this ………… day of <Month>, 2023.

____

Signature of Authorized Signatory

Name & Title of signatory:

On behalf of [Firm's name]:

<Firm's Seal>

Annexure B: Format for Earnest Money Deposit (EMD) & Bid Securing Declaration

Annexure B.1: Format for EMD

(BG from Nationalized / Scheduled Banks on Rs. 100/- Stamp Paper)

Date: _______________

To

Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

WHEREAS M/s <Name of the Bidder>, having its registered office at <-----address--> hereinafter called "the Bidder", has submitted its proposal for "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Mode",

AND WHEREAS it has been stipulated by you in the said RFP (Request for Proposal) document that the Bidder shall furnish Bank Guarantee issued by any Nationalized / Scheduled bank, for the sum of INR 100,00,000 (Rupees One Crore Only), specified therein as security for compliance with the bidder's obligations in accordance with the RFP;

AND WHEREAS we <Name of the Bank>, hereinafter referred to as "the Bank" have agreed to give the Bidder a guarantee.

THEREFORE WE, the Bank, hereby affirm that we are Guarantors and responsible to you, on behalf of the Bidder, up to a total of INR 100,00,000 (Rupees One Crore Only), and we undertake to pay you, upon your first written demand declaring the Bidder to be in default under the terms and conditions of the RFP and without cavil or argument, any sum or sums within the limit of INR 100,00,000 (Rupees One Crore Only), without your needing to prove or to show the grounds or reasons for your demand or the sum specified therein.

This guarantee should be valid for at least 30 (thirty) days post expiry of the bid validity period and shall be governed and construed in accordance with Indian Laws. The bid security amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.

Signature and Seal of Guarantors

____

____

Date:

Address:

Annexure B.2: Bid Securing Declaration for MSMEs

<on the Letterhead of the bidder>

<Date>

To

Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

I/We, The undersigned, declare that:

I/We understand that, according to your conditions, bids must be supported by a Bid Securing Declaration.

I/We accept that I/We may be disqualified from bidding for any contract with you for a period of one year from the date of notification if I am /We are in a breach of any obligation under the bid conditions, because I/We:

a. have withdrawn/modified/amended, impairs, or derogates from the tender, my/our Bid during the period of bid validity specified in the form of Bid; or
b. have been notified of the acceptance of our Bid by the purchaser during the period of bid validity
    i. fail or refuse to execute the contract, if required, or
    ii. fail or refuse to furnish the Performance Security, in accordance with the instructions to Bidders.

I/We understand that this Bid Securing Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the earlier of

i. the receipt of your notification of the name of the successful Bidder; or
ii. thirty days after the expiration of the validity of my/our Bid.

Signed: (*insert signature of person whose name and capacity are shown***)**

in the capacity of (*insert legal capacity of person signing the Bid Securing Declaration***)**

Name: (*insert complete name of person signing the Bid Securing Declaration*)

Duly authorized to sign the bid for an on behalf of: (*insert complete name of Bidder***)**

Dated on ____________________________ day of _________________________ (insert date of signing)

Corporate Seal (where appropriate)

Annexure C: Format for Performance Bank Guarantee

(To be executed on stamp paper of appropriate value)

Ref: ___________________________ Date: ____________________

Bank Guarantee Number: ____________________

To
Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

1. Against contract vide Advance Acceptance of the Tender No.__________dated_____________ covering ____________________(hereinafter called the said “Contract”) entered into between Software Technology Parks of India (STPI) (hereinafter called "the Purchaser") and___________________________________ (hereinafter called the “Bidder”), this is to certify that at the request of the Bidder, we ______________________ Bank Ltd., are holding in trust in favor of the Purchaser, the amount of___________________________________(Write the sum here in words) to indemnify and keep indemnified the Purchaser against any loss or damage that may be caused to or suffered by the Purchaser by reason of any breach by the Bidder of any of the terms and conditions of the said contract and/or in the performance thereof. We agree that the decision of the Purchaser, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by the Purchaser shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Purchaser.
2. We _______________________________Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfilment in all respects of the said contract by the Bidder i.e. till __________________hereinafter called the said date and that if any claim accrues or arises against us, ____________________Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us_______________________ Bank Ltd, notwithstanding the fact that the same is enforced within six months after the said date, provided that notice of any such claim has been given to us,___________________________ Bank Ltd, by the Purchaser before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Purchaser.
3. It is fully understood that this guarantee is effective from the date of the said contract and that \we______________________________ Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of the Purchaser.
4. We undertake to pay to the Purchaser any money so demanded notwithstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal. The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the Bidder shall have no claim against us for making such payment.
5. We________________________ Bank Ltd, further agree that the Purchaser shall have the fullest liberty, without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Tendered from time to time or to postpone for any time of from time to time any of the powers exercisable by the Purchaser against the said Bidder and to forebear or enforce any of the terms and conditions relating to the said contract and we, ________________________Bank Ltd, shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Bidder or for any forbearance by the Purchaser to the said Bidder or for any forbearance and or

omission on the part of the Purchaser or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

6. This guarantee will not be discharged due to the change in the constitution of the Bank or the Bidder.

Date: __________________________ Signature: _____________________

Place: __________________________ Printed name: _________________

Witness: ________________________

Annexure D: MSP Pre-Qualification Criteria

1. Financial Turnover

<Declaration by the statutory auditor/CA >

Date: DD/MM/YYYY

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model

Dear Sir,

This is to certify that the Annual Turnover of M/S <Registered name of bidder > from the ICT/ITeS/Data Centre/Cloud related services as per books and records for the following financial years are as under.

#	Financial Year	Annual Turnover (in INR Crores)
1	FY 2019-20	
2	FY 2020-21	
3	FY 2021-22	
	Average Annual Turnover	

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name:

Designation:

Address:

Telephone & Fax:

E-mail Address:

Instructions

1. The Bidder shall attach copies of the Balance Sheets and Profit & Loss Statements for the Financial Years 2019-20, 2020- 21 and 2021-22

2. The financial statements shall:

a. Be audited by a statutory auditor/CA.

b. Correspond to accounting periods already completed and audited (no statement for partial period shall be requested or accepted).

2. Financial Net worth

<Declaration by the statutory auditor/CA >

Date: DD/MM/YYYY

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model.

Dear Sir,

This is to certify that the Annual Turnover of M/S <Registered name of bidder > from the ICT/ITeS/Data Centre/Cloud related services as per books and records for the following financial years are as under.

#	Financial Year	Annual Net worth (in INR Crores)
1	**FY 2019-20**	
2	**FY 2020-21**	
3	**FY 2021-22**	
Average Annual Net worth (in INR Crores)		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name:

Designation:

Address:

Telephone & Fax:

E-mail Address:

3. Experience of establishing Data Centres projects

<<To be provided on the letterhead of the MSP>>

Date:

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Experience of setting up Rated 3 or above data centre for participating in RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model.

Dear Sir,

It is certified that we, M/S ………………………….. <Registered name and its communication address>, have designed, built, commissioned, and installed……… <insert number> Tier III or above certified Data Centre with 24x7x365 NOC in India, for own company or for a client and the project setup (go live date/s) is/are more than ……. years old with …………… order value/project value.

Project Details:

#	**Items**	**Bidder's Response**
1.	Name of the Entity	
2.	Assignment Name	
3.	Name of the Client	
4.	Country	
5.	Contact Details of the Client *(Contact Name, Address, TelephoneNumber)*	
6.	Approximate Value of the Contract	
7.	Duration of Assignment (*in months*)	
8.	Award Date (*month/year*)	
9.	Completion Date (*month/year*)	
10.	Narrative Description of the Project	
11.	Number of Racks commissioned	
12.	Server Farm area and Total Area in Sq. ft	

#	**Item**	**Bidder's Response**
1.	Name of the Entity	
2.	Assignment Name	
3.	Name of the Client	
4.	Country	
5.	Contact Details of the Client *(Contact Name, Address, Telephone Number)*	
6.	Approximate Value of the Contract in INR	
7.	Duration of Assignment (*in 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 tothe requirement	
12.	Documentary Evidence(s) Attached	
13.	Data Centre Power Capacity (in Megawatts / KW)	
14.	Data Centre Storage Capacity (in Peta bytes)	

Designation of the Authorized Signatory of the MSP

Date:

<To be provided each project separately on Bidder's/CSP's Letter head>

4. Data Centre Experience In case of NDA clients

<<To be provided by CA >>

Date: DD/MM/YYYY

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Experiences for participating in “RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model”.

Dear Sir,

a) It is certified that M/S …………………………. <MSP’s Registered name and its communication address>, have completed …………………………. < no of project> projects and…………………………. < insert no of projects> are going on of more than INR ……. values of each project with scope covering IT/Non-IT implementation of Data Centre Infra during last five years as on bid submission date in India.

And/or

b) It is certified that we, M/S …………………………..<MSP’s Registered name and its communication address>, have designed, built, commissioned, and installed…………………<insert number> rated-3 or above certified Data Centre with 24x7x365 NOC in India, for own company or for a client and the project setup (go live date/s) is/are more than five years old with at least INR ………order value/project value.

I further certify that I am competent officer in to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name:

Designation:

Address:

Telephone & Fax:

E-mail Address:

Note: This is applicable for the MSP, in case of NDA signed with the client.

5. MSP declaration for IT Act

<<To be provided by MSP on its Letterhead and signed by Authorized Signatory>>

Date:

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Compliant for IT act 2000 declaration in RFP for "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model".

Dear Sir,

It is certified that, M/S………………………<Registered name of the bidder and its communication address>, is compliant with IT Act 2000 (including 43A) and amendments.

Yours Sincerely,

(Authorized Signature)

Name of the Bidder:

Place:

Date:

Company Seal:

6. MSP Power of Attorney to Authorize Signatory

<To be issued on the MSP's Letterhead>

POWER OF ATTORNEY

Know all persons by these presents, we …………………………….………...…… (Name of the company) incorporated under the laws of India and having its registered office at …………………..........…………………………………………………...………… (Registered address) ["Bidder"] do hereby irrevocably constitute, nominate, appoint, and authorize Mr./Ms……….(Name), son/daughter/wife of …….……….and presently residing at ………...…………………………….., who is presently employed with us and holding the position of, as our true and lawful attorney (hereinafter referred to as the "Attorney") to do in our name and on our behalf, all such acts, deeds, matters and things as are necessary or required in connection with or incidental to submission of our Bid titled "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model" a Request for Proposal (RFP) issued by Software Technology Parks of India (STPI) and subsequently for our selection as Successful Bidder including but not limited to signing and submission of all bids and other documents and writings, participate in meetings and providing information and/or responses to STPI, representing us in all matters before STPI, signing and execution of all contracts including the Authorization Agreement and undertakings consequent to acceptance of our bid, and generally dealing with STPI in all matters in connection with or relating to or arising out of our bid for the said project and/or upon award thereof to us and/or till the entering into of the Authorization Agreement with the STPI.

AND we hereby agree to ratify and confirm all acts, deed, matters and things lawfully 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.

Capitalized terms not defined herein shall have the meaning assigned to them under the Tender Documents issued by STPI.

IN WITNESS WHEREOF ………………………………., THE ABOVE-NAMED PRINCIPAL HAS EXECUTED THIS POWER OF ATTORNEY ON THIS ………. …………DAY OF TWO THOUSAND TWENTY-THREE.

For ………………………Accepted

(Signature) ……………………………….

(Name, Designation & Address) -----------------------------------

(Signature)

(Name, Designation & Address of the Attorney)

Witness:

Instructions regarding Power of Attorney:

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 submitted under common seal affixed in accordance with the required procedure.

7. MSP experience for Internal Projects

<<To be provided on the letterhead of the MSP >>

Date:

To
Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Sub: IT/non-IT implementation experiences of Data Centre Infra for participation in RFP of the STPI titled "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model"

Dear Sir,

It is certified that we, M/S ………………………….. *<Registered name and its communication address>*, have completed at least ………………………….. < no of project> projects and………………………….. < insert no of projects> are going on of INR 50 crores values of each project with scope covering IT infrastructure implementation of Data Centre Infra during last three years as on bid submission date in India.

Project Details are given below:

#	**Items**	**Bidder's Response**
1.	Name of the Entity	
2.	Assignment Name	
3.	Name of the Client	
4.	Country	
5.	Contact Details of the Client *(Contact Name, Address, Telephone Number)*	
6.	Approximate Value of the Contract	
7.	Duration of Assignment (*in 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(s) Attached if any	

Yours faithfully,

____

Name & Designation of the Authorized Signatory

Date:

Note: Provide details of every project (For Internal project only)

8. MSP declaration for not being blacklisted

<<To be printed on MSP's Letterhead and signed by Authorized Signatory>>

Date:<insert date>
Place:<insert place>

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Dear Sir,

Subject: Declaration of Ineligibility for Corrupt or Fraudulent Practices or Blacklisted with any of the Government Agencies

I / We, Proprietor/ Partner(s) / Director(s) of M/S. __________ hereby declare that the firm/company namely M/s. ___________, as on the date of bid submission, has not been blacklisted or debarred in the last three years and is not under blacklisting period /active debarred list by STPI or any of the Central or State Government Organization / Public Sector Undertaking / Autonomous Body etc.

In case the above information is found false I/We are fully aware that the tender/ contract will be rejected/ cancelled by STPI and execution of Bid Securing Declaration. In addition to the above STPI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

OR

I / We Proprietor/ Partner(s)/ Director(s) of M/S. _____________ hereby declare that the firm/company namely M/S_________________ in the last three years, was blacklisted or debarred by STPI, or any other Central or State Government Organization / Public Sector Undertaking / Autonomous Body etc. for a period of _____ months /years w.e.f. _____. The period is over on _____ and, as on the date of bid submission the firm /company is not in active blacklisting period and now entitled to take part in Government tenders.

In case the above information is found false I/We are fully aware that the tender/ contract will be rejected/cancelled by STPI and execution of Bid Securing Declaration. In addition to the above STPI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

Yours truly,

<Signature>

<Name in Block Capitals>

<Designation>

<Company name with address, contact number and e-mail address>

<Company Seal>

Annexure E: Compliance sheet for qualification

#	Pre-qualification Criteria	Documentary Evidence Required	Provided (Yes/No)	Reference Page No.
1.	Legal Entity	Copy Certificate of Incorporation issued by Registrar of Companies, PAN, GSTN certificate, CIN, Copy of IT Return, Office registration certificate.		
2.	Annual Turnover	Three years audited financial statements AND Auditor's certificate (2019-20, 2020-21 & 2021-22)		
3.	Net Worth	Three years audited financial statements AND Auditor's certificate (2019-20, 2020-21 & 2021-22)		
4.	Project Experience	Experience details with documentary evidence for scope of work and contract value, along with client contact details, in the form of Work order / Purchase order / Completion certificate from client Declaration by authorized signatory of the Bidder for internal project		
5.	Data Centre Establishment Experience	Experience details with documentary evidence for scope of work and contract value, along with client contact details, in the form of Work order / Purchase order / Completion certificate from client Declaration by authorized signatory of the Bidder for internal project		
6.	NoC/SoC Experience	Declaration by authorized signatory of the Bidder		
7.	Blacklisted Entity / Debarment for MSP	Declaration by authorized signatory of the Bidder		
8.	Authorized Signatory	Board Resolution / Power of Attorney		
9.	Earnest Money Deposit	EMD in the form of BG or Bid securing declaration (in case of MSME)		
10.	Office in India	Declaration from bidder for having permanent office in India		

#	Pre-qualification Criteria	Documentary Evidence Required	Provided (Yes/No)	Reference Page No.
11.	No Deviation and undertaking Total Responsibility	Declaration by authorized signatory of the Bidder		
12.	Deployment Model	MSP will provide Architecture and solution design for Cloud services delivery models 1. Hybrid Cloud Deployment 2. GCC deployment		
13.	Cloud management layer	MSP will provide Cloud management layer for Integration, orchestration, Automation and self-service portal		
14.	Security	MSP shall provide Cybersecurity, Data Security and SOC solution including a. Security SOC tools and SOC implementation for internal security b. Data Security		

Annexure F: CSP Pre-Qualification forms

1. CSP's Auditor's Certificate for Avg. Annual Turnover

<Declaration by the statutory auditor/CA >

Date: DD/MM/YYYY

To

Tender Division,
Software Technology Parks Of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

Subject: RFP for "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model"

Dear Sir,

This is to certify that the Annual Turnover of M/s…………………….. <Registered name of CSP> from cloud related services as per books and records for the following financial years are as under.

S. No.	Financial Year	Annual Turnover (in cr.)
1	2019-20	
2	2020-21	
3	2021-22	
Average Annual Turnover		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name:

Designation:

Address:

Telephone & Fax:

E-mail Address:

Instructions

The Bidder shall attach copies of the Balance Sheets and Profit & Loss Statements for the Financial Years 2019-20, 2020- 21 and 2021-22.

The financial statements shall:

a. Be audited by a statutory auditor/CA;
b. Correspond to accounting periods already completed and audited (no statement for partial period shall be requested or accepted).

2. Format for Information about CSP's Rated-3 Data Centres

<<To be printed on CSP's Letterhead and signed by Authorized Signatory>>

Date: _______________

To

Tender Division,
Software Technology Parks Of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

Subject: Data Centre Details for participating in RFP of STPI titled "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model"

Dear Sir,

It is certified that we, M/s……………………<Registered name of the CSP and its communication address> have Data Centres from where in Public Cloud services will be offered is currently in operation in India and have following number of operational racks

Type	Complete address (with contact email and phone numbers	Number of operational racks
Primary Data Centre		
Secondary (DR) Data Centre		

The said Data Centres have the following IT infrastructure operational:

- Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centres, Backup, Operations Management, and Data Management
- Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

They are at least Rated- 3 standard Data Centre. #They are also preferably certified under TIA 1942 or uptime institution certifications by a 3rd party, namely M/s ______________________ <insert name of certifying agency>#

Yours faithfully,

Name & Designation of the Authorized Signatory of the CSP

Date:

# - Strike out if not certified by any third-party agency #

3. CSP’s Managed Services Format

<<To be printed on CSP’s Letterhead and signed by Authorized Signatory>>

Date: _______________

To,

Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

Subject: Participation in RFP of the STPI titled “RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model”.

Dear Sir,

It is certified that we, M/s ………………………<Registered name of the CSP and its communication address>, have an operational public cloud/managed services on cloud and all services mentioned in this RFP are available through our self-service portal.

We hereby confirm that the cloud services offered by the …………………………………<Insert name of the CSP> are fully compliant to the technical specifications for cloud services/solutions defined in the RFP.

Yours faithfully,

____

Name & Designation of the Authorized Signatory of the CSP

Date:

4. CSP's Declaration for not being Blacklisted / Debarred

<<To be printed on CSP's Letterhead and signed by Authorized Signatory>>

Date:<insert date>

Place:<insert place>

To

Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

Subject: Declaration of Ineligibility for Corrupt or Fraudulent Practices or Blacklisted with any of the Government Agencies

Dear Sir,

I / We, Proprietor/ Partner(s) / Director(s) of M/S. __________ hereby declare that the firm/company namely M/s. ___________, as on the date of bid submission, has not been blacklisted or debarred in the last three years and is not under blacklisting period /active debarred list by STPI or any of the Central or State Government Organization / Public Sector Undertaking / Autonomous Body etc.

In case the above information is found false I/We are fully aware that the tender/ contract will be rejected/cancelled by STPI and execution of Bid Securing Declaration. In addition to the above STPI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

or

I / We Proprietor/ Partner(s)/ Director(s) of M/S. _____________ hereby declare that the firm/company namely M/s_________________ in the last three years, was blacklisted or debarred by STPI, or any other Central or State Government Organization / Public Sector Undertaking / Autonomous Body etc. for a period of _____ months /years w.e.f. _____. The period is over on _____ and, as on the date of bid submission the firm /company is not in active blacklisting period and now entitled to take part in Government tenders.

In case the above information is found false I/We are fully aware that the tender/ contract will be rejected/cancelled by STPI and EMD shall be forfeited. In addition to the above, STPI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

Yours truly,

<Signature>

<Name in Block Capitals>

<Designation>

<Company name with address, contact number and e-mail address>

<Company Seal>

5. CSP declaration for IT Act

<<To be provided by CSP on its Letterhead and signed by Authorized Signatory>>

Date:

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Compliant for IT act 2000 declaration in RFP for "Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model".

Dear Sir,

It is certified that, M/S……………………..<Registered name of the bidder and its communication address>, is compliant with IT Act 2000 (including 43A) and amendments.

Yours Sincerely,

(Authorized Signature)

Name of the Bidder:

Place:

Date:

Company Seal:

6. CSP Authorization Format (CAF)

<<To be printed on CSP's Letterhead and signed by Authorized Signatory>>

Date:

To

Tender Division,
Software Technology Parks of India, 1st Floor, Plate B,
Office Block - 1, East Kidwai Nagar,
New Delhi – 110023
Tel: 011-24628081/24346600
Email – cloudrfp@stpi.in

Subject: Authorization for participating in RFP for "Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model".

Dear Sir,

It is certified that we, M/S..*<Registered name of the CSP and its communication address*>, having cloud services facilities in India at *<Cloud Location(s)*>, do hereby authorize M/s ....*<Registered name of the Bidder (MSP) and its communication address*> to participate and submit a bid against the RFP as referred above.

We hereby confirm that the cloud services offered by the ………………………………….. <Insert name of the CSP> are fully compliant to the technical specifications for cloud services/solutions defined in the RFP.

We herewith certify that the hybrid cloud service offered as part of project scope are not end of life/end of support and we hereby undertake to support these services for the duration of minimum 123 months from the date of go live of cloud services.

Yours faithfully,

____

Name & Designation of the Authorized Signatory CSP

Date:

7. CSP Power of Attorney to Authorize Signatory

<To be issued on the CSP's Letterhead>

POWER OF ATTORNEY

Know all persons by these presents, we ……………………………….…………...…… (Name of the company) incorporated under the laws of India and having its registered office at …………………...........…………………………………………………...………… (Registered address) ["CSP"] do hereby irrevocably constitute, nominate, appoint, and authorize Mr./Ms……….(Name), son/daughter/wife of …….….……and presently residing at ………...…………………………….., who is presently employed with us and holding the position of, as our true and lawful attorney (hereinafter referred to as the "Attorney") to do in our name and on our behalf, all such acts, deeds, matters and things as are necessary or required in connection with or incidental to submission of our Bid titled "RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model" a Request for Proposal (RFP) issued by Software Technology Parks of India (STPI) and subsequently for our selection as Successful Bidder including but not limited to signing and submission of all bids and other documents and writings, participate in meetings and providing information and/or responses to STPI, representing us in all matters before STPI, signing and execution of all contracts including the Authorization Agreement and undertakings consequent to acceptance of our bid, and generally dealing with STPI in all matters in connection with or relating to or arising out of our bid for the said project and/or upon award thereof to us and/or till the entering into of the Authorization Agreement with the STPI.

AND we hereby agree to ratify and confirm all acts, deed, matters and things lawfully 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.

Capitalized terms not defined herein shall have the meaning assigned to them under the Tender Documents issued by STPI.

IN WITNESS WHEREOF …………………………………, THE ABOVE-NAMED PRINCIPAL HAS EXECUTED THIS POWER OF ATTORNEY ON THIS …………………... DAY OF TWO THOUSAND TWENTY-THREE.

For ………………………Accepted

(Signature) ……………………………….

(Name, Designation & Address) -----------------------------------

(Signature)

(Name, Designation & Address of the Attorney)

Witness:

Instructions regarding Power of Attorney:

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 submitted under common seal affixed in accordance with the required procedure.

Annexure G: List of Services

Below services need to be delivered from STPI Data Centres by on-prem setup of required hardware, software, and support services.

Quantity mentioned is usable capacity dedicated for customer workloads. Bidder may propose the quantities required for any overhead for running orchestration solution, virtualization or any other component required to run this solution.

A1) List of services to be offered from the Hybrid Cloud setup & GCC

#	Service Name	Type of Services	Unit of measure
A	**Compute Services**		
1	VM (With OS options - Windows, Linux, Ubuntu LTS, RHEL etc)	IAAS	Per VM / Hour
4	Add On Options – RAM upgrade, vCPUs Upgrade	NA	As applicable
B	**Storage Services**		
1	Block Storage - SSD - 100 GB minimum 50 to 250 IOPS	IAAS	Per GB Storage / Hour
2	Block Storage - HDD - 100GB minimum 50 to 250 IOPS	IAAS	Per GB Storage / Hour
4	Backup Storage – 100GB	IAAS	Per GB Storage / Hour
5	SMB for Windows storage SSD– 100 GB	IAAS	Per GB Storage / Hour
6	NFS storage – 100GB SSD	IAAS	Per GB Storage / Hour
7	Object storage – 100GB	IAAS	Per GB Storage / Hour
8	Low-cost object storage -100 GB	IAAS	Per GB Storage / Hour
C	**Network Services**		
1	Bandwidth Lease Line (Internet/Intranet)	IAAS	Per 100 Mbps
2	NAT gateway	IAAS /PAAS	Throughput in Mbps
3	VPN (site to site) each connection supporting 10 sites	IAAS	Per VPN Connection / Month
4	VPN (client site) each connection supporting 120 clients	IAAS	Per VPN Connection / Month
D	**Security Services**		

#	Service Name	Type of Services	Unit of measure
1	Application load Balancer	IAAS/PAAS	Throughput in Mbps
2	Next Gen Firewall	IAAS/PAAS	Throughput in Mbps
3	WAF	IAAS/PAAS	Throughput in Mbps
4	HSM - 10 Keys	IAAS	No of Keys /Month
5	SSL certificate	IAAS	Per Certificate / Month
E	**Database Services**		
1	Postgres – Can range from min. 2 vCPUs to max. 64 vCPUs	PAAS	Per VM / Hour
2	MySQL - Can range from min. 2 vCPUs to max. 64 vCPUs	PAAS	Per VM / Hour
3	MS SQL (Enterprise) - Can range from min. 2 vCPUs to max. 64 vCPUs	PAAS	Per VM / Hour
4	MongoDB Can range from min. 2 vCPUs to max. 64 vCPUs	IAAS	Per VM / Hour
5	Redis - Can range from min. 2 vCPUs to max. 64 vCPUs	IAAS /PAAS	Per VM / Hour
6	NoSQL DB – Can range from min. 2 vCPUs to max. 64 vCPUs	IAAS/PAAS	Per VM / Hour
F	**Container Services**		
1	Kubernetes - 1 Worker Node	PAAS	Per VM / Hour
2	Kubernetes - 1 Master Node (Can be provided from Public Cloud)	PAAS	Per VM / Hour
3	Kubernetes Cluster Management Service (Can be provided from Public Cloud)	PAAS	Per Cluster/Hour
G	**Other Services**		
1	Back-up as a service	PAAS	Per GB /month
2	DR as a service	PAAS	Per Instance / Month
3	Data Migration as a Service – per 100 GB	PAAS	Instance + Storage / Month
4	Database Migration as a Service – per 100GB Source and Destination as same DB type	PAAS	Storage/activity
5	Database Migration as a Service – per 100GB	PAAS	Storage/Activity

#	Service Name	Type of Services	Unit of measure
	Source and Destination as diff DB types		
6	Resource optimization and cost management	PAAS	Node/Activity

A2) List of specialized services

Below services may be provided by the CSP from its Public Cloud

#	Service Name	Type of Services	Unit of measure
A	**Network Services**		
1	API gateway (throughput 2500 Mbps)	PAAS	No. API Request / Month
2	DNS service	PAAS	No of DNS Queries(millions) / month
3	Egress Bandwidth	IAAS	Per Mbps / Month
4	CDN	PAAS	Per GB data egress / Month
5	Load balancer – network	IAAS	Throughput in Mbps
6	Public IP	IAAS	IP/Month
B	**Security Services**		
1	Multi-factor authentication - 100 Identities	IAAS	Per User / Month
2	SIEM - 500 EPS	IAAS	EPS
3	MDM - 100 Devices	IAAS	Per Device /month
4	DDOS (Layer 3 & 4)	PAAS	Throughput in Mbps
5	DDOS Layer 7	PAAS	Throughput in Mbps
6	Vulnerability scanning - 100 Devices /IPS	IAAS	Instance scanned / Month
7	Anti-malware - 100 Devices	IAAS/PAAS	Per License Per VM / Month
8	KMS - 10 Keys	PAAS	No of Keys /Month
C	**Database Services**		
1	Hadoop (committed usage for 1 year) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour
2	Casandra (committed usage for 1 year) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour
3	Hadoop (committed usage for 3 year) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour

4	Casandra (committed usage for 3 year) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour
5	Hadoop (on-demand usage) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour
6	Casandra (on-demand usage) - 16 vCPU: 128 GB RAM	PAAS	Per VM/hour
D	**Messaging Service**		
1	Kafka - 4vCPU: 16 GB RAM (2 nodes)	PAAS	Per VM / Hour
E	**Other Services**		
1	Serverless	PAAS	/GB sec; per req
2	Video Streaming Service	PAAS	Instance/ GB / Month
3	Email as a Service	PAAS	Per Mailbox(50GB)/month
4	Email as a Service	PAAS	Per Mailbox(100GB)/month
5	Messaging Service	PAAS	Per Msg GW/Month
6	Cloud Infrastructure, service, and workload monitoring.	PAAS	Per Node/Month
7	BOT Service	PAAS	As Applicable
8	Machine Learning Service	PAAS	As Applicable
9	AI Service	PAAS	As Applicable
10	Cognitive Services	PAAS	As Applicable
11	Devops	PAAS	As Applicable
12	Lab Services	PAAS	As Applicable
13	Load Testing Services	PAAS	As Applicable
14	Blockchain Service	PAAS	As Applicable

Note: Selected MSP shall provide an online published catalogue for each service offered. The catalogue shall include detailed information about the service, including its features, benefits, pricing, and any relevant terms and conditions. The catalogue prices shall be comparable to the market rate. There will be committee consisting of members from the selected MSP and STPI team which will finalise the rate card of the services offered and will be reviewed on a "Yearly" basis. However, in case of addition of new service, the inclusion and deliberation of the rate can be done at any point of time in the existing rate card

Annexure H: Technical Specification

The CSP need to provide the compliance to the technical specification of each of the services as per the format mentioned in this section on its letter head. The MSP shall also conter sign the compliance sheet.

1. GCC Infrastructure

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1.	GCC infrastructure shall be designed for high availability with dual redundancy for all solution components to enable reliable auto recovery workflows.			
2.	Cloud services running locally on GCC shall be upgraded seamlessly without affecting the services or users and in consultation with STPI.			
3.	GCC platform should support cloud native Infrastructure services, API, and tools to work seamlessly on-premises.			
4.	Cloud platform should have service available to build secure and compliant GCC architectures.			
5.	Cloud platform should have single provisioning layer to manage workloads running on different technology stacks (Openstack, VMware, Microsoft, Nutanix etc). Any services delivered via GCC infrastructure shall have the same consistent user experience, console, configuration on cloud services offered via different technology stacks in future.			
6.	The cloud infrastructure / services provisioned by the MSP must support elasticity. The end-users should be able to scale out workload (compute/storage/network/databases/applications/security etc.) on-demand within on-premises and other GCC sites in case resources in on-premises cloud is fully utilized.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
7.	GCC infrastructure should be a fully managed service supported by MSP. Offered solution should provide single console to manage workloads. Offered solution should provide a native migration and disaster recovery service to move workloads to other GCC sites.			
8.	It must provide infrastructure, APIs, services, and tools wherever applications may need to reside to meet low latency, local data processing, or data residency requirements.			
9.	The infrastructure should be delivered, installed, monitored, patched, and updated to meet the required SLAs.			
10.	MSP shall ensure that offered solution should provide a necessary billing solution to provide monthly /quarterly billing details for end users and STPI. Necessary provision to provide email/SMS notification on billing details should be available in the offered solution. MSP should be able to automate invoices and billing reports to STPI and respective tenants over the email. Cloud platform should be able to automate invoices and billing reports to STPI and respective tenants over the email.			
11.	Necessary 24 x 7 help desk services for grievance redressal will be setup and provided by MSP.			
12.	All necessary monitoring tools to ensure effective monitoring, smooth functioning of the GCC infrastructure setup and associated support infrastructure should be made available by the MSP. SLA for the offered cloud services/applications/workloads provided to the end-user and SLA for the GCC infrastructure setup, will be monitored by monitoring tools provided by MSP.			
13.	All necessary hardware required for smoothly running the GCC infrastructure and SLA compliance needs to be provisioned by the MSP including but not limited to MPLS and Internet bandwidth and its associated hardware, landing points, security components etc.			
14.	Before the Go-Live of Services from on-premises, a comprehensive UAT for the hardware, GCC platform, services, workloads will be conducted. Bidder to provide sample UAT reports. All the necessary tools and services required for the conduct of UAT shall be provided by the MSP.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
15.	Before the Go-Live of services from the GCC setup, the bidder has to conduct a comprehensive security audit including VAPT. 3rd party agency conducting the audit should be certified and should certify a zero-gap security report. MSP will appoint the 3rd party agency upon approval of STPI. Cost of the audit to be taken care by the MSP.			
16.	Go-Live of services from GCC setup will be announced after successful UAT, successful demo of the cloud solution and zero gap security audit report.			
17.	MSP should arrange 3rd party (certified agency) security audits every six months and submit a certified zero gap report for the same. MSP will appoint the 3rd party agency upon approval of STPI. Cost of the audit to be taken care by the MSP.			
18.	Peripheral physical security and security guards for STPI Data Centres will be provided by STPI. The MSP shall ensure the security and maintenance of the area utilized by the MSP for IT infrastructures at all locations.			
19.	The MSP should provide all variants of cloud service as per MeitY guidelines. • Infrastructure as a Service (IaaS), • Platform as a Service (PaaS) • Software as a Service (SaaS)			
20.	Offered cloud solution must be scalable. The end user shall be able to add/expand or scale out/up the infrastructure in future on demand basis.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
21.	The cloud infrastructure / service provisioned by the MSP must support elasticity. The end-users should be able to scale out (automatically and manual) workloads (compute/containers/kubernetes/storage/network/databases/applications/security etc.) on-demand.			
22.	No prior intimation or buffer will be given to scale up or scale out the services/workloads/applications. Scale up or scale out should happen automatically based on the controls/parameters set up for maximum/minimum usage of VMs.			
23.	All the services (IaaS, PaaS & SaaS) offered by MSP from GCC should support pay as you consume model.			
24.	Proposed cloud solution should come with its own / 3rd party backup solution with ransomware protection functionality.			
25.	Services, workloads, hardware, and its components not limited to servers, storage, switches, routers, firewalls, load-balancers etc. hosted on GCC should be able to integrate with NTP server of STPI or NPL for synchronization.			
26.	MSP should provide the audit logs of the complete environment including but not limited to servers, storage, SAN switches, network switches, routers, security/firewall appliances, services IaaS/SaaS/PaaS, operating systems etc.			
27.	GCC platform should provide the functionality to protect data from accidental deletion for the period of 3 months.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
28.	GCC platform should be able to provision any service in less than 15 minutes from the time of request.			
29.	Proposed GCC infrastructure should provide confidential computing to protect data in use by encrypting data in memory and processes. Encryption should support integration with the HSM (on-premises hardware) for key management.			
30.	Cloud platform should offer availability of 99.9% or higher for the complete architecture and its individual workloads, services, applications & resources.			
31.	On-premises cloud should have minimum uplink capability of 100 G or above with provision of future expansion as and when required.			
32.	On-premises hardware proposed for cloud platform must be designed in line with maximum power feed of per rack capacity available at STPI Data Centre.			
33.	On-premises hardware and cloud platform should have power saving functionality to reduce power consumption. Power consumption should be proportional to the consumption of workloads and services.			
34.	GCC platform should have minimum 10% GPU based servers for specialized workloads like AI/ML and Big Data.			

1. Hybrid Cloud Infrastructure

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1.	Hybrid cloud infrastructure shall be designed for high availability with dual redundancy for all solution components to enable reliable auto recovery workflows.			
2.	Cloud services running locally on Hybrid cloud shall be upgraded seamlessly without affecting the services or users and in consultation with STPI to the latest version in line with the services offered in public cloud.			
3.	Cloud platform should support cloud native Infrastructure services, API, and tools to work seamlessly on-premises and public cloud.			
4.	Cloud platform should have service available to build secure and compliant hybrid cloud architectures.			
5.	Cloud platform should have single provisioning layer to manage on-premises workloads and public cloud workloads. Any service delivered on hybrid cloud infrastructure shall have the same consistent user experience, console, configuration on both on-premises and public cloud services offerings.			
6.	Cloud platform should be able to provide fully managed service that offers the same cloud infrastructure, services, APIs, and tools to any datacentre, co-location space or on-premises facility for a truly consistent hybrid experience. The infrastructure should be delivered, installed, monitored, patched, and updated by CSP/MSP.			
7.	The cloud infrastructure / services provisioned by the MSP must support elasticity. The end-users should be able to scale out workload (compute/storage/network/databases/applications/security etc.) on-demand within on-premises and public cloud in case resources in on-premises cloud is fully utilized.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
	All services provided as per scope of this RFP should be available on public cloud also (provided by CSP). Burst out to public cloud should only be done, when the on-premises resources setup by the MSP in STPI's DC are fully utilized or as decided by STPI stakeholders.			
8.	On premises infrastructure should be a fully managed service and supported by CSP/MSP. Offered solution should provide single console to manage on-premises workloads and public cloud workloads. Offered solution should provide a native migration and disaster recovery service to move workloads to hybrid cloud. Services such as DBaaS on hybrid cloud should patch both OS and database engines within scheduled maintenance windows with zero downtime.			
9.	It must provide infrastructure, APIs, services, and tools wherever applications may need to reside to meet low latency, local data processing, or data residency requirements.			
10.	The infrastructure should be delivered, installed, monitored, patched, and updated to meet the required SLAs.			
11.	MSP shall ensure that offered solution should provide a necessary billing solution to provide monthly /quarterly billing details (on-premises & public cloud) for end users and STPI. Necessary provision to add project details & provide billing details should be available in the offered billing solution. Necessary provision to provide email/SMS notification on billing details should be available in the offered solution. MSP should be able to automate invoices and billing reports to STPI and respective tenants over the email. Cloud platform should be able to automate invoices and billing reports to STPI and respective tenants over the email.			
12.	Necessary 24 x 7 help desk services for grievance redressal will be setup and provided by MSP.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
13.	All necessary monitoring tools to ensure effective monitoring, smooth functioning of the cloud infra setup and associated support infrastructure should be made available by the MSP. SLA for the offered cloud services/applications/workloads provided to the end-user and SLA for the cloud infrastructure setup on-premises/public cloud will be monitored by monitoring tools provided by MSP.			
14.	All necessary hardware required for smoothly running the on-premises cloud infrastructure and SLA compliance needs to be provisioned by the MSP including but not limited to MPLS and Internet bandwidth and its associated hardware, landing points, security components etc.			
15.	Before the Go-Live of Services from on-premises, a comprehensive UAT for the hardware, cloud platform, services, workloads will be conducted. Bidder to provide sample UAT reports. All the necessary tools and services required for the conduct of UAT shall be provided by the CSP/MSP.			
16.	Before the Go-Live of services from on-premises cloud setup, the bidder has to conduct a comprehensive security audit including VAPT. 3rd party agency conducting the audit should be certified and should certify a zero-gap security report. MSP will appoint the 3rd party agency upon approval of STPI. Cost of the audit to be taken care by the bidder.			
17.	Go-Live of services from on-premises cloud setup will be announced after successful UAT, successful demo of the cloud solution and zero gap security audit report.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
18.	MSP should arrange 3rd party (certified agency) security audits every six months and submit a certified zero gap report for the same. MSP will appoint the 3rd party agency upon approval of STPI. Cost of the audit to be taken care by the MSP.			
19.	Peripheral physical security and security guards for STPI Data Centres will be provided by STPI. The MSP shall provision the required resources for security and maintenance of the area utilized by the MSP for IT infrastructures at all locations.			
20.	The CSP should provide native marketplace with certified applications which can be deployed on cloud. The CSP should also provide capability for administrators to create private marketplace with images from the public marketplace. Marketplace should be a digital catalogue that provides access to 3rd party services which are validated for policy, security, compliance, software vulnerabilities and product usability.			
21.	The CSP should provide all variants of cloud service as per MeitY guidelines. • Infrastructure as a Service (IaaS), • Platform as a Service (PaaS) • Software as a Service (SaaS)			
22.	MSP should own the unified SLA for the entire cloud platform (On-premises and public). For On-premises unified SLA should include underlying hardware, cloud platform, services, workloads, and any other components.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
23.	MSP should offer hybrid cloud in a manner that if an application developed using the on-premises setup, STPI should be easily able to migrate the same to cloud without doing any application modifications, re-coding, re-building, API calls etc.			
24.	Offered cloud solution must be scalable. The end user shall be able to add/expand or scale out/up the infrastructure in future on demand basis.			
25.	The cloud infrastructure / service provisioned by the MSP must support elasticity. The end-users should be able to scale out (automatically or manual) workload (compute/containers/kubernetes/storage/network/databases/applications/security etc.) on-demand within on-premises and public cloud (in case resources in on-premises cloud is fully utilized).			
26.	No prior intimation or buffer will be given to scale up or scale out the services/workloads/applications. Scale up or scale out should happen automatically based on the controls/parameters set up for maximum/minimum usage of VMs.			
27.	All the services (IaaS, PaaS & SaaS) offered by MSP from on-premises or public cloud should support pay as you consume model.			
28.	Proposed cloud solution should come with its own / 3rd party backup solution with ransomware protection functionality.			
29.	Proposed cloud solution should be able to support and run virtual machines/instances/Kubernetes/containers/databases from same cloud platform.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
30.	Services and workloads hosted on public cloud should be able to integrate with NTP server of STPI or NPL for synchronization.			
31.	Services, workloads, hardware, and its components not limited to servers, storage, switches, routers, firewalls, load-balancers etc. hosted on Hybrid cloud should be able to integrate with NTP server of STPI or NPL for synchronization.			
32.	MSP should provide the audit logs of the complete environment including but not limited to servers, storage, SAN switches, network switches, routers, security/firewall appliances, services IaaS/SaaS/PaaS, operating systems etc.			
33.	Cloud platform should provide the functionality to protect data from accidental deletion for the period of 3 months.			
34.	Cloud platform should be able to provision any service in less than 15 minutes from the time of request.			
35.	Cloud platform through its provisioning layer should be able to connect, orchestrate and provision heterogenous cloud environments like AWS, Azure, GCP, oracle, open stack, OpenShift etc.			
36.	Proposed on-premises and associated public cloud infrastructure should provide Confidential computing to protect data in use by encrypting data in memory and processes. Encryption should support integration with HSM (on-premises hardware) for key management.			

#	**Requirements**	**Compliance (Y/N)**	**Reference** **(Document/ Page No.)**	**Remarks / Deviation** **(if any)**
37.	Cloud platform should offer availability of 99.9% or higher for the complete architecture and its individual workloads, services, applications & resources.			
38.	On-premises cloud should have minimum uplink capability of 100 G or above with provision of future expansion as and when required.			
39.	On-premises hardware proposed for cloud platform must be designed in line with maximum power feed of per rack capacity available at STPI Data Centre.			
40.	On-premises hardware and cloud platform should have power saving functionality to reduce power consumption. Power consumption should be proportional to the consumption of workloads and services.			

2. Hybrid Cloud Provisioning and Management Layer

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1.	Cloud platform should have cloud-provisioning portal both control plane and data plane for multiple tenants to provide automation and orchestration of resources for on-premises and public cloud and should support multifactor authentication for login for all the tenants.			
2.	Cloud should help manage the interaction between cloud consumers and providers. Key cloud management functions required include service enablement; monitoring and observation; and provisioning and orchestration.			
3.	Self-service portal should be able to provide visibility to the catalogue of services offered by STPI to the end client.			
4.	Self-service portal should integrate seamlessly with orchestration layer of the hybrid cloud infrastructure.			
5.	Self-service portal should generate necessary SLA reports and reports should be made available to end clients via email.			
6.	Self-service portal layer should help enforce policies and controls to ensure compliance with best practices of cloud activity. Self-service portal should support Key cloud management functions which should include but not limited to identity management, security, governance multi-level approval etc.			
7.	Cloud provisioning layer should support multi-tenancy and resource pooling for all the services or applications.			
8.	Cloud provisioning layer should have its own automation service and should support integration with 3rd party automation tools.			
9.	Cloud Provisioning layer should support but not limited to RESTful APIs and WebSocket APIs to enable integration with any 3rd party hybrid cloud management software/platform.			
10.	Cloud platform should provide IaaS, PaaS & SaaS services. Complete list of services provided in scope of work section.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
11.	Proposed solution should have single console to manage on-premises workloads and public cloud workloads. Any service delivered on hybrid cloud infrastructure shall have the same consistent user experience, console, configuration, and billing unit of measure on-premises and on public cloud.			
12.	Cloud platform should be able to failover with entire or partial workload to disaster recovery site and failback with entire or partial workload to Data Centre site.			
13.	Cloud platform should be able to failover with entire or partial workload to public cloud and failback with entire or partial workload to on-premises.			
14.	MSP should ensure minimum RTO of 60 mins and RPO of 15 mins in case of failover to DR site or public cloud.			
15.	Cloud platform should have its own monitoring solution to monitor entire cloud infrastructure including workloads & services with an integrated helpdesk tool for automated ticketing.			
16.	Cloud platform should have a SIEM solution to monitor entire cloud infrastructure including workloads & services and should be able to provide SIEM as a Service for end customers.			
17.	MSP should have capability to provide insights about the access, usage etc. with a dashboard. Usage and metering of both on-premises and public cloud needs to be consolidated on a single dashboard.			
18.	MSP should ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.			
19.	Cloud platform should support IPV4 & IPV6 for all the services which will be provisioned from on-premises or public cloud for all the tenants.			
20.	Cloud platform should be able to provide metering and billing service of all on-premises and public cloud services like VMs, Storage, and Managed Databases etc. at per minute granularity.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
21.	MSP should provide various pricing option such as on-demand, one or three-year committed pricing for services consumed from public cloud.			
22.	Self-service portal should be integrated with payment gateway (origin within India) to enable payment modes like UPI gateways and credit cards. MSP to propose the list of payment gateways originating from India, STPI will approve the payment gateway to be integrated.			

3. Compute

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide completely managed compute service for all the tenants from GCC, on-premises cloud and public cloud			
2	Capability to provision virtual machines/container workload over API calls without any manual intervention.			
3	Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.			
4	Configuration and management of the virtual machine shall be enabled via a Web browser over SSL VPN/Secure tunnel as against the public internet.			
5	In case of suspension of a running VM or container, the VM shall still be available for reactivation for reasonable time (90 days) without having to reinstall or reconfigure the VM for the Client solution.			
6	MSP to perform periodic patching of complete cloud platform as per the SLAs and KPIs mentioned.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
7	Cloud service architecture should be in such a way that it avoids VM outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level.			
8	All the VMs/Instances should have 1:2 ratio of physical to virtual core only.			
9	Physical CPU in the cloud platform should be under support from CSP/MSP/OEM during the entire contract duration. Any tech refresh/upgrade/replacement required during the contract period to ensure compliance is to be undertaken by the bidder without causing disruption to existing workloads, within the stipulated SLA and at no cost to STPI or end customers. Any products offered to STPI should not be refurbished or reused.			
10	GCC, On-premises and public Compute instances should provide network capability of 1G, 10G and 25G.			
11	RHEL OS should be with 24x7 premium subscription. Ubuntu OS on IaaS should be LTS with enterprise support and once LTS is coming to end bidder needs to update the OS.			
12	Bidder will upgrade the operating system if and when operating system is reaching end of support cycle.			

3. Block Storage

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Block Storage should be available on GCC, On-Premise and public cloud for all the tenants.			
2	Block storage should provide different classes or high IOPS workload & for archival requirements based on the performance for different workloads.			
3	Block Storage service should have the feature to take the backup of the block volume by taking snapshots. Feature should have the functionality for snapshot to be created or deleted automatically using custom schedule. Block storage should be able to replicate between DC and DR and between on-premises and public cloud.			
4	Block storage should allow to create storage volumes and attach them to VMs/instances/Kubernetes containers/Kubernetes clusters.			
5	The managed storage should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine, without having to provision a new volume, copy/move the data.			
6	Block volumes should support replication to another on-premises facility or to the public cloud.			
7	Block volumes should provide the availability of 99.9% or higher.			
8	For the proposed Block Storage, CSP should offer the capability to increase the Volume size in minimum increments of 5GB or lower so that charges are for the actual usage.			
9	Block storage should support seamless encryption (AES-256 cryptographic algorithm), on data volumes, boot volumes, disk I/O and snapshots. Encryption service should support integration with 3rd party key manager or cloud's inbuild key manager.			

4. File Storage

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide a fully managed file storage for both windows and Linux workloads.			
2	File storage service should be available from both on-premises and public cloud for all the tenants			
3	File storage should provide availability of 99.9% or higher			
4	File storage should preferably offer multiple classes for different sets of data viz. frequently access data and non-frequently access data.			
5	File storage should have feature of implementing aging policy on the files stored to save the space based on the criteria defined by the department.			
6	File storage should support NFS 4.0 and latest version for Linux workloads.			
7	The Managed Storage should have capability to increase storage capacity on demand on the provisioned shares without any reboot of the virtual machine/instance			
8	File storage should provide encryption for data at rest and data in transit.			
9	File storage should have capability to integrate with VMs/Instances/Containers/Kubernetes & serverless services.			
10	File storage should support seamless encryption (Data at rest), on files and folders stored in the share. Encryption service should support integration with 3rd party key manager or cloud's inbuild key manager.			

5. Object Storage

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide object storage for all the tenants from both on-premises and public cloud for all the tenants.			
2	Object storage service should provide parallel access to objects stored in the storage.			
3	Object storage should provide functionality to replicate either to another on-premises facility or to public cloud.			
4	Object storage should provide Write Once Read Many locks feature on the objects stored.			
5	Object should provide multiple storage classes for multiple uses according to performance.			
6	Proposed object storage should support versioning, where multiple versions of an object can be kept in one store. Versioning should protect against unintended overwrites and deletions.			
7	Proposed object storage should offer encryption of data ‘at-rest’, i.e., data stored on volumes and snapshots and ‘in-transit’. Encryption feature should be enabled by default.			
8	Proposed object storage should offer object storage automated tiering capability, i.e., the ability to recommend transitioning an object between object storage classes based on its frequency of access			
9	Proposed object storage should Support multi-factor authentication (MFA) for various operations as an additional security option			
10	Cloud service should support flexible access- control policies to manage permissions for objects			
11	Object storage should support seamless encryption (Data at rest), on objects. Encryption service should support integration with 3rd party key manager or cloud’s inbuild key manager.			
12	Object storage should provide the availability of 99.9% or higher.			

6. Database

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide database as a service for all the tenants from GCC, on-premises and public cloud for all the tenants.			
2	Cloud platform should provide managed database service for (relational) databases like MongoDB, MS-SQL, MySQL, PostgresDB from GCC, on-premises infrastructure and from public cloud.			
3	CSP should provide managed database Service that supports Self Service Public API's for managing database functions including Start/Stop, Back-Up, restoration, Configuration and Scaling.			
4	Managed database should support high availability and synchronous/asynchronous replication and automatic failover of a primary database to a standby database in a separate physical data centre or to public cloud to improve data redundancy.			
5	Managed database should support automatic or manual scale out to other on-premises cloud platform or to public cloud.			
6	Managed database service should offer encryption of data 'at-rest' and 'in-transit'			
7	Databases provisioned should be up-to date with latest patches.			
8	Database service should offer multiple classes of storage for different workloads as per different performance levels.			
9	Database service should support scalability of database instances to add resources like CPU/Memory and storage.			
10	CPU should be scalable to 64vCPUs			
11	Memory should be scalable to 256GB RAM			

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
12	Storage – Should be scalable to 16TB within one file system on the fly without reboot of the instance.			
13	Read only Replica should have the feature to increase the read performance by automatic scaling out of read only instances of the databases and offloading read queries to read only instances. (All the database types mentioned above).			
14	Database should provide the backup and restore functionality to provide the point in time recovery for database instance. It should do backup of database and transaction logs up to defined retention period (up to 30 days). Restore functionality should allow to restore the instance to any second during the retention period.			
15	Database should offer encryption (at rest and in transit) to encrypt the databases through the keys managed by 3rd party key manager or cloud platform inbuilt key manager.			
16	All the Instances should have 1:2 ratio of physical to virtual core only.			
17	Bidder will provide all operating systems and databases. All the DBs should be with enterprise support.			
18	Bidder will upgrade the operating system and database software if and when operating system and database is reaching end of support cycle. Patching and upgradation of operating system and/or databases should preferably be automated. CSP/MSP to provide a report every month to all customers and STPI mentioning details for all the OS and/or databases requiring upgrade. Upgrading and patching should preferably be done without any downtime. If downtime is mandatory than relevant ITSM process and procedures should be followed.			
19	Databases can be provisioned from the CSP’s marketplace.			

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
20	MSP/Bidder can propose SSD or NVMe drives with an option to dynamically change the IOPS for all kinds of database workloads.			

7. Containers and Kubernetes

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
1	Cloud platform should provide fully managed containers and Kubernetes cluster services from on-premises and public cloud for all the tenants.			
2	For container services controller nodes could be provisioned in public cloud, but worker nodes should be on-premises.			
3	Container Service should allow creation of both windows and Linux containers.			
4	Container Service should offer docker to create and run a multi-container service/application			
5	Container Service should have its own repository with container images and should allow integration with 3rd party repositories.			
6	Container Service should automatically recovery unhealthy containers.			
7	Container Service should allow to define rules to manage scalability.			
8	Container Service should allow to integrate with integrated file storage for persistent storage.			
9	Container Service should support Docker networking and integrates with cloud tenant(virtual) network to provide isolation for containers			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
10	Container service should support integration with cloud platform's inbuilt load balancing service, allowing to distribute traffic across containers using Application Load Balancers or Network Load Balancers. Service should automatically add and remove containers from the load balancer			
11	Container service should provide monitoring capabilities for containers and clusters through its own monitoring service or third-party monitoring service.			
12	Kubernetes service should be certified Kubernetes-conformant, so existing applications that run on upstream Kubernetes are compatible with proposed Kubernetes service in the cloud platform.			
13	Kubernetes service should automatically manage the availability and scalability of the Kubernetes control plane nodes responsible for scheduling containers, managing application availability, storing cluster data, and other key tasks.			
14	Kubernetes service should allow integration with networking services like load balancers, security services, identity services for RBAC.			
15	Kubernetes service should provide scalable and highly available Kubernetes control plane between different on-premises facilities or public cloud.			
16	Kubernetes service should provide an integrated console for Kubernetes clusters. Cluster operators and application developers can use Kubernetes service console as a single place to organize, visualize, and troubleshoot Kubernetes applications running on the proposed cloud platform.			
17	Kubernetes service should let tenant create, update, scale, and terminate nodes for cluster with a single command.			
18	Kubernetes service should support windows as well as Linux nodes for master and worker services.			
19	Kubernetes service should support isolation between 2 different Kubernetes clusters running for a single tenant within the same network.			
20	Kubernetes service should allow to isolate the traffic on bases of IP addresses and TCP/UDP ports.			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
21	All the Instances should have 1:2 ratio of physical to virtual core only.			
22	Container platform to be deployed should be available or portable across multiple cloud providers with enterprise support for ease of application migration.			
23	Container platform should be able to run other CNCF compliant Kubernetes cluster used by STPI.			
24	Container platform should have service mesh and provide container native persistent storage in on-prem cloud infrastructure and public cloud infrastructure.			

8. DNS

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide fully managed, highly available and scalable cloud domain name service from on-premises or public cloud.			
2	DNS service should provide recursive DNS for tenant's virtual and on-premises networks and resolving all STPI related queries.			
3	DNS service should guard recursive DNS queries and should allow to build firewall rules that filter DNS traffic against these rules.			
4	DNS should be a single unified service for both on prem and public cloud.			

9. Load Balancer

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide the fully managed load balancing service to distribute incoming application and network traffic across multiple targets, such as instances, containers, Kubernetes cluster, IP addresses, and serverless service from on-premises or public cloud for all the tenants.			
2	Load balancing service should handle load of your network and application traffic with in on-premises and public cloud.			
3	Load balancing service should provide gateway load balancers, network load balancer and application load balancer			

10. Next Generation Firewall

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide fully managed next generation network firewall to protect all the resources tenant will use from GCC, on-premises or public cloud for all the tenants.			
2	Next generation firewall service should be available from GCC, on-premises or public environment both and should be scalable for all the tenants.			
3	Next generation firewall should allow to define rules that give granular control over network traffic			
4	Next generation firewall service should offer built-in redundancies to ensure all traffic is consistently inspected and monitored.			
5	Next generation firewall Service should provide availability of 99.9%.			
6	Next generation firewall service should permit to scale up or down capacity based on the traffic load.			

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
7	Next generation firewall should be stateful firewall to achieve granular policy enforcement.			
8	Next generation firewall should have intrusion detection and prevention feature.			
9	Next generation firewall service should provide all the logs for alert and traffic flow and should allow to store the logs in cloud platform's object or file storage service.			
10	Next generation firewall service should allow centralized management and deployment of security policies across all applications and virtual networks.			
11	Next generation firewall service should have features like URL filtering, application filtering, SSL offloading, decryption capabilities and integration with vault service to safeguard critical information(secrets).			

11. VPN

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
1	Cloud platform should provide highly available and fully managed VPN (site to site & Client) service from GCC, on-premises and public cloud for all tenants.			
2	Site to site service should create encrypted tunnels between tenants on-premises network and cloud platform.			
3	Client VPN should allow users to connect to cloud platform using VPN software client.			
4	Client VPN should authenticate using Active directory/LDAP or certificates			

12. WAF

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available and fully managed WAF service to protect applications and APIs for all the tenants from GCC, on-premises or public cloud for all the tenants.			
2	WAF service should allow to create rules to filter web traffic based on various conditions.			
3	WAF service should allow to create rules that block common web exploits like SQL injection and cross site scripting.			
4	WAF service should allow re-usability of rules that can be deployed across multiple websites or applications.			
6	WAF should allowed to be completely managed via APIs.			
7	WAF should provide real-time metrics.			
8	WAF should integrate with monitoring solution inbuilt in the cloud platform or any 3rd party monitoring solution.			

13. CDN Services

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should have highly available, fully managed, and scalable content data network service for all the tenants from public cloud to provide data, videos, applications, and API			

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
2	CDN service should deliver content, APIs or applications over HTTPS using the latest version Transport Layer Security (TLSv1.3) to provide end to end encryption and secure communication.			
3	CDN service should support more than one origin for backend architecture redundancy.			
4	CDN service should provide ability for protection against Network and Application Layer Attacks.			
5	CDN service should provide ability to restrict access only to authenticated viewers.			
6	CDN should be integrated with the Storage service, for easy access of documents/data using CDN			
7	Cloud platform should provide application load balancer to distribute the traffic across many computing resources within the same site to increase the responsiveness and availability of applications.			

14. DDOS

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide fully managed, scalable, and highly available DDOS service from GCC, on-premises or public cloud for all tenants and its own platform.			
2	DDOS service should provide always-on detection and automatic inline mitigations that minimize application downtime and latency			
3	DDOS service should provide comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks, applications, and website attacks.			
4	DDOS service should provide detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with Cloud platform's web application firewall.			
5	DDOS service should provide a dedicated response team and protection against DDoS related spikes in VMS/instances, load balancers, CDN and DNS.			
6	DDOS service should provide always-on network flow monitoring, which inspects incoming traffic to cloud services and applies a combination of traffic signatures, anomaly algorithms, and other analysis techniques to detect malicious traffic in real time			
7	DDOS service should provide customized detection based on traffic patterns to protect elastic IP addresses,			
8	DDOS should use the health of your applications to improve responsiveness and accuracy in attack detection and mitigation			
9	DDOS should provide complete visibility into DDoS attacks with near real-time notification using monitoring solution inbuilt with cloud solution or 3rd party monitoring solution			

15. Identify and Access Management

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed Identity and access management, service from GCC, on-premises or public cloud for all tenants			
2	Access management service should provide granular access control,			
3	Access management service should allow to delegate access to users.			
4	Access Management service should provide attribute-based access control			

16. API Gateway

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed API gateway service from on-premises or public cloud for all tenants			
2	API gateway service should allow to create Restful APIs using either HTTP APIs or REST APIs. HTTP APIs are the best way to build APIs that do not require API management features.			

17. HSM Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed dedicated HSM service from on-premises and public cloud for all tenants			
2	HSM service should provide access to HSMs that comply with the FIPS 140-2 Level 3 standard for cryptographic modules and RSA 2048-bit sign/verify.			

18. Key Management Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, scalable KMS service from on-premises or public cloud for all tenants			
2	KMS service should provide centralized control over the lifecycle and permissions of your keys.			
3	KMS service should allow services to encrypt data at rest, or to facilitate signing and verification using a KMS key			

19. Certificate Manager

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, scalable certificate manager service from on-premises or public cloud for all tenants			
2	CM service should allow to easily manage SSL/TLS certificates.			
3	CM service should provide managed private CA service.			

20. Kafka

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, scalable Kafka service from on-premises or public cloud for all tenants			
2	Kafka service should allow to create a fully managed Kafka cluster that follows Kafka’s deployment best practices or create your own cluster using a custom configuration.			
3	Kafka service should have zookeeper included to cluster tasks and maintain state for resources interacting with the cluster.			

21. Backup as a Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, scalable backup service from GCC, on-premises or public cloud for all tenants and for all workloads and services.			
2	Backup service should offer a centralized management console. Console can run from the public cloud; however, backup target should be present in on-premises cloud.			
3	Backup service should allow to create backup policies that enable to define backup requirements and then apply them to the cloud resources, workloads, services you want backed up. It should allow to create separate backup policies that can meet specific business and regulatory compliance requirements, helping to ensure that each of cloud resources, workloads, services are backed up and protected			
4	Backup service should allow to create customized backup schedules to meet business and regulatory backup requirements			
5	Backup policy should allow to set backup retention policies that will automatically retain and expire backups according to the business and regulatory backup compliance requirements.			
6	Backup service should provide ransomware protection for its workloads, services.			
7	Backup service should provide monitoring dashboard to monitor running backup and restore activities and to view completed or failed backup job logs.			
8	Backup service should provide lock mechanism to protect backups from deletion or changes to their lifecycle by unintended or intended changes			
9	Bidders to configure backup policies as per the RTO/RPO requirements of the application in discussion with the end user.			

22. DB Migration as a Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, scalable DB migration service from on-premises or public cloud for all tenants and for multiple database types			
2	DB migration service should allow to migrate data to and from most of the widely used commercial and open-source databases.			
3	DB migration service should allow both homogeneous (same DBs) migrations as well heterogenous databases (Different databases).			
4	DB migration service should allow migrations to and from IaaS to Database as a Service, both homogenous and heterogenous migrations.			

23. Resource Optimization and Cost Management

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, predictive workload optimization service from GCC, on-premises or public for all tenants for all the workloads, services etc.			
2	Optimization service should analyse the configuration and resource utilization of your workload and recommend how the workload would have performed on various configurations and provide cost benefits to the customer.			

24. Messaging Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, messaging service from on-premises or public for all tenants.			
2	Messaging service should allow tenants to connect with their clients/users/tenants over channels like email, SMS, push, voice, or in-app messaging			

25. Monitoring Service

#	**Requirements**	**Compliance (Y/N)**	**Reference (Document/ Page No.)**	**Remarks / Deviation (if any)**
1	Cloud platform should provide highly available, fully managed, monitoring service from GCC, on-premises or public for all tenants (all the workloads – on-premises/public) and for the on-premises hardware on which cloud platform is deployed.			
2	Monitoring service should collect and store logs from GCC, on-premises/ public cloud hardware, workloads, resources, applications, and services in near real time			
3	Monitoring service should have a dashboard through which tenants can view and create reusable graphs and visualize on-premises hardware, cloud resources, workloads, and applications in a unified view.			
4	Monitoring service should send alerts and alarms and allow to combine the alerts and alarms to reduce number of alarms in case one issue is affecting many resources, workloads, or services.			
5	Monitoring service should provide actionable insights for all GCC and on-premises hardware, resources, workloads, services etc. to provide insight into health.			
6	Monitoring service should be able to store and analyse the logs for the period of 10 years within GCC and on-premises setup.			
7	Monitoring service should offer a dashboard that displays up-to- the minute information on service availability across DC and DR and public cloud.			

26. Auditing Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any)
1	Cloud platform should provide highly available, fully managed, Always On auditing service from GCC, on-premises or public for all tenants (all the workloads – GCC, on-premises/public for multiple accounts) and for the on-premises hardware on which cloud platform is deployed.			
2	Auditing service should allow delivery and storage of events to any file or object storage available in the cloud platform.			
3	Audition service should allow delivery of logs or events to government agencies for auditing and forensics.			
4	Auditing service should be available and enabled by-default without any manual intervention or start of services.			
5	Auditing service should also allow delivery and storage of logs for ongoing events as well.			
6	Auditing service should encrypt all the logs before being stored to object storage, file storage or before sending it to govt agencies. It should allow integration with cloud in-built key managed service and/or any 3rd party key manager service used by the tenant.			

27. Application Performance Management Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any
1	Cloud platform should provide highly available, fully managed, APM service from GCC, on-premises or public for all tenants (all the applications – on-premises/public for multiple accounts)			
2	APM service should support applications running on IaaS(compute), containers, Kubernetes and serverless platform.			
3	APM Service should provide end-to-end, cross-service view of requests made to application.			
4	APM service should support tracing for applications that are written in multiple language such as but not limited to Node.js, Java, and .NET			

28. Serverless Compute

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any
1	Cloud platform should provide highly available, fully managed, serverless compute from on-premises or public cloud for all tenants (multiple accounts).			
2	Serverless compute service should run the code in response to events and automatically manages the underlying compute resources for tenants.			
3	Serverless service should allow tenants to use any third-party library, framework, SDKs etc			
4	Serverless service should support Java, Go, PowerShell, Node.js, .NET, Python, and Ruby code, and provide a Runtime API allowing tenant to use any additional programming languages to author functions.			

5	Serverless service should manage all the infrastructure to run code on highly available, fault tolerant infrastructure and update the underlying operating system (OS) when a patch is released.			
6	Serverless service should automatically scale up or out the underlying infrastructure when the usage grows.			

29. SIEM as a Service

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any
1	Cloud platform should provide highly available, fully managed, SIEM as a Service from on-premises or public cloud for all tenants and for cloud platform including its hardware and all other components.			
2	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action	s		
3	Next Generation SIEM with security analytics capabilities shall be integrated with all devices in the Data Centre, DR site, systems, application, and end-user devices. SIEM shall be integrated with application logs of target application for end-to-end security monitoring.			
4	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.			
5	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources			
6	The SIEM solution should be based on open architecture so that it can be used to feed data to 3rd party analytic solutions			
7	The SIEM solution support high availability feature and should be proposed in HA mode for all layers at DC			
8	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is			

#	Requirements	Compliance (Y/N)	Reference (Document/ Page No.)	Remarks / Deviation (if any
	processed. Log Filtering needs to be available across all tiers to filter out logs as wherever required.			
9	SIEM solution must support OOB of the box integration with well-known technologies e.g., firewall, AD, Switches, routers, TI etc. for creating response to an incidence			
10	Should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow. Collectors must support integration with N Flow, Jflow			
11	The solution should have connectors to support the listed devices / applications. In case device is not supported out of box it must have GUI Based SDK kit to create Parsers.			
12	All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission. No performance degradation should happen.			
13	The solution should have the capability to compress the logs for storage optimization.			
14	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system. License count should be performed post filtering of logs.			
15	The solution should be able to store both normalized and RAW logs			
16	Solution should have the ability to perform free text searches for events, incidents, rules, and other parameters.			
17	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users			
18	The proposed solution must be capable of processing and storing large volumes of historical log data (10 Years) that can be restored and analysed for forensic investigation purposes.			

30. Automation Service

#	**Requirements**	**Compliance (Y/N)**	**Reference** **(Document/ Page No.)**	**Remarks / Deviation** **(if any**
1	Cloud platform should provide highly available, fully managed, automation Service from on-premises or public cloud for all tenants and for cloud platform including its hardware and all other components.			
2	Automation service should be agnostic to any kind of operating system.			
3	Automation service should support to automate the tasks in one or many hosts simultaneously.			
4	It should support REST API and CLI for integration with other tools			
5	Provide capability to define workflow for multiple automation jobs			
6	Should be capable of automating the deployment or administration of VMs, instances, containers, Kubernetes clusters, storage, network, databases etc.			
7	Automation solution should be able to automate STPISI's existing DC stack like VMware, Open stack, Hyper-V, firewalls and other security systems like, IPS/IDS, network devices(multi-OEM).			
8	Automation solution should support creation of workflows and manage exception handling along with management of inventory in on-premises and public cloud.			
9	Automation solution should be agnostic to any cloud, hardware, security, databases, network etc. and should integrate with cloud infrastructure running at STPI DCs and its associate public cloud.			

31. API Management Service

#	**Requirements**	**Compliance (Y/N)**	**Reference** **(Document/ Page No.)**	**Remarks / Deviation** **(if any**
1	Cloud platform should provide highly available, fully managed API management Service from on-premises or public cloud for all tenants and for cloud platform.			
2	API management service should support complete API lifecycle			
3	It should have API gateway component which shall act like façade to backend services			
4	API management service must support REST & WebSocket requests, rate limiting and minimum of 5GB of In-Memory Cache.			
5	The API Gateway must not need any provisioning of servers and it must include all hardware and other components required to deliver the service			
6	The managed API gateway should provide a turnkey solution for publishing APIs to external and internal consumers. It should support following capacity (sizing) : HTTP API Calls - 300 M / monthly, REST API Calls 300 M / monthly, API Caching - up to 5GB, WebSocket API Calls - 1B / monthly.			
7	It should have Automated/Push button scaling with published APIs for scaling so that developers can create custom logic to scale the application as per business requirements.			
8	It should have API projection via API keys and application authorisation tokens			
9	It should provide built-in API developer portal (via automatic deployment) that enables API customer to discover the API and use them			
10	It must offer (or integrate with) observability features of the cloud platform to monitor resources, APIs and applications.			

32. Additional Compliance Requirements

#	**Requirements**	**Compliance (Y/N)**	**Reference** **(Document/ Page No.)**	**Remarks / Deviation** **(if any**
1	The proposed architecture and solution design for Cloud services delivery models Hybrid Cloud Deployment GCC Deployment			
2	Cloud management layer should be capable of Integration, orchestration, Automation and self-service portal for both GCC and Hybrid Cloud deployment.			
3	Cybersecurity, Data Security and SOC solution including Security SOC tools and SOC implementation for internal and Data Security			
4	The proposed cloud solution must have Scalable and Burstable architecture along with the methodology for moving from Private Cloud to Public Cloud and vice versa			

Annexure I: Demonstration Plan

Bidder shall demonstrate/submit documentary proof for POC (Proof of Capability) as part of technical evaluation to understand the key features such as AUTO Scale up/down, Security protocols, Denial of Service (DoS, DDoS) attack), management and administration and audit capabilities for offerings, setting up of DR facilities, etc.

S. No.	Demo Capability to be shown	Public URL
1	Demonstration data lake services for customers using CSP service offered tools and services	
2	Demonstrate cost analysis and optimization (Including actual tools, services and steps for cost analysis)	
3	Demonstrate cloud foundation and landing zone that supports development, operation, and governance of the use cases.	
4	Demonstrate the billing and cost calculator services.	
5	Demonstrate the CSP Support capability by logging a ticket and showcase the interaction with the support engineer to resolve the issue	
6	Demonstrate the scaling up and down of capacity for the DBaaS (Serverless database) without interrupting the application	
7	Demonstrate querying data stored in Data Lake and OLTP [Postgres] database from Data warehouse interface.	
8	Demonstrate features of ETL/ELT pipelines with a focus on enterprise scale: a. ETL/ELT pipeline parameterization to process a group of files in a single pipeline. b. Scalability of the ETL/ELT pipeline implementation to reflect changes in data volume, job concurrency and related factors while minimizing impact on response time on a job-by-job basis. . c. Showcase ELT by ingesting data from Postgres database to Data warehouse. Integration of pipelines with metadata management, data lineage, and data catalogue services.	
9	Demonstrate out of the box functionality of data analytics including: a. ML/AI automation scripting: demonstrate by example the ability to streamline ML/AI workflows using scripting or other techniques to reduce effort of iterative tasks in end-to-end	

S. No.	Demo Capability to be shown	Public URL
	analytics processes including model development, training, and operationalization. b. Model lifecycle management: demonstrate by example the steps of analytics model development and use of the model including version control, team collaboration, and evaluation of model performance. Capabilities to enable tagging/labelling of model related parameters for the purposes of enabling management and administration of model creation, administration and use.	
10	Demonstrate by example how a non-IT user can perform self-service: a. Preparation of input data, b. visual analytics, c. automated model building, and Promotion of a model to a production environment.	
11	Demonstrate querying data lake for setting up a Public/Population Dashboard using Cloud native business intelligence tool. Bidder must use anonymized datasets for this demo.	

The bidder should be ready to demonstrate on their proposed cloud before the Tender Evaluation Committee through the following use cases.

S No.	Use Case
1	Demonstrate cloud foundation and landing zone that supports development, operation, and governance of the use cases. Specifically, the Proponent should: 1. Create an organizational master account (root account) with full security controls to only manage the master and provide access to business unit administrator. The master account should only provision and manage member accounts at the organization level as user Acc-1 2. Using master account, create a business unit account with access to essential functions common to all the accounts under the Organization, such as log archive, security management, and shared services like the directory service and CI/CD pipeline services. 3. Using a business account, create 2 business product accounts including: a. An account with access to the CI/CD pipeline with user Dev-1. b. A deployment account with user Bus-1 for operation, monitoring and management of a sample workload. 4. Using the business unit account, create isolated “sandboxes” or developer accounts for individuals learning and experimentation, as a best practice. Maximum points will be awarded where the Proponent demonstrates all of 1 through 4 above through a service management console.
2	The bidder should demonstrate the billing and cost calculator services by: 1. Demonstrating the bidder proposed cost calculator with configuration based on the configuration of cloud services as configured in UC2 for the sample workload deployment. The demonstrated cost calculator should explicitly illustrate: a) The configuration of used cloud services including infrastructure, container and DBaaS related services. b) The capability for recommendation of optimized configuration to minimize cost for the target workload. 2. Demonstrating the billing and cost management services by demonstrating: a) Setting a monthly budget based on the provided cost calculator b) Setting alert thresholds 3. Demonstrating the cost and service dashboards indicating current period costs and billing. Maximum points will be awarded where the Proponent demonstrates all of 1 through 4 above through a service management console.

S No.	Use Case
3	Demonstrate the CSP Support capability by logging a ticket and showcase the interaction with the support engineer. Evaluation committee can log a support ticket under any service/category for evaluation purpose. Specifically, the bidder should demonstrate: 1. What are the support options available and how to access them? 2. How to enable support? 3. Log a ticket in real-time under a category [evaluation committee will share the category under which support case needs to be logged at the time of demo] 4. Showcase how the support conversations flows.
4	The bidder should demonstrate the scaling up and down of capacity for the DBaaS (Relational Serverless database) without interrupting the application. The bidder should demonstrate how the application platform service can be configured and scaled through a service management console demonstrating: 1. How DBaaS environments [Serverless database] scales; 2. Configuration options in database console that can be configured for database scaling; 3. The bidder should demonstrate by generating load on the database and showcase DBaaS dashboards indicating activity across the execution of the use case. Maximum points will be awarded where the bidder demonstrates containers and DBaaS configuration options including all of 1 through 3 above through service configuration management, monitoring and/or dashboard screens accessed through the service management console.
5	Demonstrate querying data stored in Data Lake and OLTP [Postgres] database from Data warehouse interface.

S No.	Use Case
6	Demonstrate features of ETL/ELT pipelines with a focus on enterprise scale: Overview: the ETL pipeline reads two source files and maps the fields to a target file. 1. Information about the source and target data files are stored in a configuration file named “mapping”, in the json/xml/yaml/hocon format - whatever works for the tool. The ETL pipeline gets the following information from the config file: a. Sources: i. source_db1, URL= db1_WHATEVER, input_db1_file1_YYYYMMDD.ext ii. source_db2, URL= db2_WHATEVER, input_db2_file2_YYYYMMDD.ext b. Target: i. target_db, URL= dB WHATEVER ii. output_db_file3_YYYYMMDD.ext c. source_db1 (any RDBMS), source_db2 (a RDBMS different from db1), target_db (any RDBMS) d. “ext”s are extension of the files based on the type of the files and RDBMS; and e. The source and target files are date stamped (YYYYMMDD), the date is a parameter in the configuration file. 2. About the files: a. There are 10 fields in file1, and 5 in file2 that are mapped to the target file file3 b. There is a common field named record_id in file1 and file2 c. There are 100 records in each of file1 and file2 such that each record in file1 matches a record in file2 with same value of record_id 3. Records of file1 that cannot be mapped to file3 because of an error during mapping, e.g., value does not match a field type, are to be rejected and written to a log file based on the target file name, e.g., file3YYYYMMDD_badrecords, with its corresponding file1 and file2 fields 4. The loading task stops if a file2 record has any error during mapping 5. Scenarios to be demonstrated: a. Data loaded successfully with no bad records b. Data loaded with 10 bad records c. Loading task fails in record 68 of file2, operator re-starts the task to load the data after a manual fix (whatever) so that the task can continue at record 68 and completes without any issue · There should not be any duplicates in file3 after this restart

S No.	Use Case
7	Demonstrates out of the box functionality for data analytics including: ML/AI automation scripting: demonstrate by example the ability to streamline ML/AI workflows using scripting or other techniques to reduce effort of iterative tasks in end-to-end analytics processes including model development, training, and operationalization. Use out of the box functionality to demonstrate automation (using script) of the following processing steps: 1. Get source data set from source: file name= sample_dataset, location = a URL a. The source data set can be any data set; the workflow/scripting is what is important b. As an example, suppose the source data has the following fields i. business_id: int ii.area_code: int 2. Load/store the source data in a non-production location (location = a URL), create two identical copies sample_data9set_org (original) & sample_dataset_wrk (working) i. Sample_dataset_org does not get modified ii. Sample_dataset_wrk is used for analysis 3. Perform some data wrangling as follows on sample_dataset_wrk: a. Remove records when sample_dataset_wrk. business_id is null b. If (area-code = blank OR null) set the area-code = 0 4. Split the total records into 2 groups, e.g., using random sampling based on area_code for training and testing 5. Build two machine learning models, e.g., logistic regression (reg_mod) and random forest (rnd_frst) or any other algorithm and show the score of each 6. Select the one with the highest score and run it against the actual data 7. Show model debugging during model training. 8. Deploy the one with the highest score to a production environment 9. Use deployed model in any sample business application. Show human review workflow for custom model to review ML output before consuming it in application. 10. Group Models based on business requirements and compare model with the help of visualizations.
8	Demonstrate by example how a non-IT user can manually perform self-service analytics including: a. preparation of input data, b. visual analytics, c. automated model building, and d. promotion of a model to a production environment. 1. A business user (User) connects to data storage in cloud. 2. User browses available datasets in the data storage and chooses a dataset. 3. User runs the query to obtain some information about the dataset using SQL and Phyton code (e.g., how many null in “ID” field, Sum of “Cost” field, and count on a “Location” field when it is “Delhi”). 4. User browses a list of pre-existing models in the repository and reviews the meta-data including use case description. 5. User searches and filter the models based on model meta-data, e.g., use case is related to Fraud. 6. User promotes a model to the production to run again against data already in production.

S No.	Use Case
9	Demonstrate querying data lake for setting up a Public/Population Healthcare Dashboard using Cloud native business intelligence tool. *Bidder must use anonymized datasets or synthetic patient data for this demo. 1. Setup a patient data store in FHIR format [10K or more dummy patient data] 2. Showcase how the data is demoralised for querying and aggregation 3. Demonstrate running SQL queries on the normalised data store. 4. Integrate the data store with business intelligence tool 5. Showcase aggregated reports/charts i. Count of records by conditions ii. Aggregation of daily patient encounters iii. Aggregation of clinical status

Annexure J: Template for Commercial Bid

<<To be printed on MSP's Letterhead and signed by Authorized Signatory>>

Date:<insert date>

Place:<insert place>

To

Tender Division,
Software Technology Parks of India,
1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi - 110023
Tel: +91-11-24628081

Subject: Revenue share of RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model"

Dear Sir,

This is to certify that M/S <Registered name of bidder > will share the Revenue% age share (R) with STPI accordingly as per the given slabs in the table.

S. No.	**Revenue earned by bidder (in Cr)**	**Weightage (%)**	**Revenue % Share to STPI (R)**
Slab 1	0-100	60	A
Slab 2	101-500	30	B
Slab 3	>500	10	C

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive. We confirm that no technical deviations are attached here with this commercial offer

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Name

Designation

Seal

Date

Place

Business Address

Annexure K: Template for CV of proposed manpower

<table>
<tr><td>1</td><td>Name of the Staff
(With PP size photo)</td><td></td></tr>
<tr><td>2</td><td>Current Designation in the Organization and Employee ID</td><td></td></tr>
<tr><td>3</td><td>Proposed Role in the Project</td><td></td></tr>
<tr><td>4</td><td>Proposed Responsibilities in the Project</td><td></td></tr>
<tr><td>5</td><td>Date of Birth</td><td></td></tr>
<tr><td>6</td><td>Education</td><td>&lt;Degree>/<Diploma>, <College/University>, <Year of Passing>, <Result Marks/Grade&gt;</td></tr>
<tr><td>7</td><td>Key Training and Certifications</td><td></td></tr>
<tr><td>8</td><td>Language Proficiency</td><td><table>
<tr><th>Language</th><th>Reading</th><th>Writing</th><th>Speaking</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>9</td><td>Employment Record
(For the Total Relevant Experience)</td><td><table>
<tr><th>From/To</th><th>Employer</th><th>Position Held</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>10</td><td>Total No. of Years of Work Experience</td><td></td></tr>
<tr><td>11</td><td>Total No. of Years of Experience for the Role Proposed</td><td></td></tr>
<tr><td>12</td><td>Highlights of relevant assignments handled and
significant accomplishments</td><td>Use following format for each project<table>
<tr><td>Name of Assignment / Project</td><td></td></tr>
<tr><td>Year</td><td></td></tr>
<tr><td>Location</td><td></td></tr>
<tr><td>Client</td><td></td></tr>
<tr><td>Main Project <b>Features</b></td><td></td></tr>
<tr><td>Position Held</td><td></td></tr>
<tr><td>Activities Performed</td><td></td></tr>
</table></td></tr>
</table>

Certification

I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes me, my qualifications, and my experience. I understand that any willful misstatement described herein may lead to my / my company's disqualification from the bidding process.

Date: __________

Place: _________

(Sign of the person/resource)

Annexure L: General information of the Bidder

<To be printed on the Company Letterhead of the Bidder>

#	Parameters	Details
1.	Name of the Firm	
2.	Registered Office address: Telephone Number: Fax Number: e-Mail Address:	
3.	Correspondence/Contact address:	
4.	GSTIN Number	
5.	PAN Number	
6.	Details of Contact Person (Name, designation, address etc.): Telephone Number: Fax Number: e-Mail Address:	
7.	Year and place of the establishment of the company	
8.	Registration Number & Registration Authority	
9.	Is the firm a • Government/Public Sector Undertaking • Proprietary/Partnership firm (*if Partnership firm, give partnership deed*) • Limited/Private Limited company or Limited Corporation • member of a Group of Companies (*give name and address, and description of other companies*) • a subsidiary of a large corporation (*give the name and address of the parent organization and state what involvement, if any, will the parent company have in this project*)	
10.	Total number of employees	
11.	Are you registered with any Government/Department/Public Sector Undertaking (*if yes, give details*)	
12.	Number of Offices/Project Locations	
13.	Do you have a Local Representation or Office in India? (*If so, please give the address of the local office*)	
14.	List the major clients with whom your organization has been/is currently associated	
15.	Were you ever required to suspend a project for a period of more than three months continuously after you started? (*If so, give the names of project and reasons for the same*)	

16.	Have you in any capacity not completed any work awarded to you? (*If so, give the name of project and reason for not completing the work*)	
17.	Have you ever been denied tendering facilities by any Government/ Department/Public sector Undertaking? (*If yes, give details*)	

Date:

Name & Signature of Authorized Representative:

Company Seal:

Name of Agency:

Full Address:

Telephone No.:

Annexure M: Details of STPI Edge locations

STPI has proposed the following edge locations to start the initial services which may be further expanded to other locations as well.

S. No.	**Centre Name**	**Total Rack Count in facility**	**Vacant Rack Count in facility (If any)**	**Total available Rack space (RU) in facility**	**Total NOC/DC area (sqft)**	**Server farm area (sqft)**	**Incoming power to facility (KVA)**	**Power backup capacity (KVA)**	**UPS Power Capacity and redundancy**
1	Pune	9	1	42 U	606 sq. ft.	76 sq. ft.	400 KVA	125 KVA	20 KVA (N + 1)
2	Kolkata	4	2	70 U	665 sq. ft.	100 sq ft	20 KVA	13 KVA (5 KVA + 8 KVA)	UPS System 1 - (2 x 10 KVA) UPS System 2 - (10 KVA)
3	Lucknow	3	119	126 U	482 sqft	Nil	90KVA	62.5 kva	4 X 10 KVA
4	Jaipur	2	1	42 U	400 Sq. Ft.	Nil	40 KVA	380 KVA DG Set	2x40 KVA (N+1)

S. No.	Centre Name	Total Rack Count in facility	Vacant Rack Count in facility (If any)	Total available Rack space (RU) in facility	Total NOC/DC area (sqft)	Server farm area (sqft)	Incoming power to facility (KVA)	Power backup capacity (KVA)	UPS Power Capacity and redundancy
5	Chennai	100	16	672	5000 sqft	3500 sqft	1.6MVA	2 numbers of 750KVA DG set and 1 number of 500 KVA DG set	2N (2 numbers of 400 KVA UPS)
6	Dehradun	1.IT Park NOC rack count-3	40 U	1.IT Park NOC rack space-(42U+36U=78U)	1.IT Park NOC area-300 Sqft	1.IT Park server farm area-50 Sqft	1.IT Park facility-80 KW	1.IT Park NOC-60 KVA 2. Survey Chowk NOC-20KVA	1.IT Park Facility-60(20X3) KVA (N+1) 2.Survey Chowk Facility-20(10X2)KVA
		2.Survey chowk NOC area-1		2.Survey chowk NOC area-36 U	2.Survey chowk NOC area-345 Sqft	2.Survey chowk NOC area-50 Sqft	2.Survey chowk facility-25 KW		

S. No.	Centre Name	Total Rack Count in facility	Vacant Rack Count in facility (If any)	Total available Rack space (RU) in facility	Total NOC/DC area (sqft)	Server farm area (sqft)	Incoming power to facility (KVA)	Power backup capacity (KVA)	UPS Power Capacity and redundancy
7	Guwahati*	3	Nil	81 U	Carpet Area - 218.8 sqft , Super Area - 373.36 sqft	Nil	18.125 KVA	UPS Power Capacity = 120 KVA , DG Power capacity= 250 KVA	UPS Power Capacity = 120 KVA

* Expansion space is available

Annexure N: Integrity Pact

INTEGRITY PACT

Between

Software Technology Parks of India (STPI), herein after referred to as **"The Principal"**,

And

…………………………………………………………. hereinafter referred to as **"The Bidder/Contractor"**

Preamble

The principal intends to award, under laid down organizational procedures, contract/s for ……………………………………. The principal 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 Contractor(s).

In order to achieve these goals, the principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section

1 – Commitments of the Principal

i. The principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

   a. No employee of the principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

   b. The principal will, during the tender process treat all Bidder(s) with equity and reason. The principal will in, before and during the tender process, provide to all Bidder(s) 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 the tender process or the contract execution.

   c. The principal will exclude from the process all known prejudiced persons.

ii. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitment of the Bids/Contractor(s)

i. The Bidder(s)/Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

a. The Bidder(s)/Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract 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 the tender process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) / Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the principal as part of the business relationship, regarding plans, technical proposals, and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents / representatives in India, if any. Similarly, the Bidder(s)/Contractor(s) 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(s) / Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative must be in Indian Rupees only.

e. The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to, or intends to make to agents, brokers, or any other intermediaries in connection with the award of the contract.

ii. The Bidder(s) / Contractor(s) will not instigate third persons to commit offences outlines above or be an accessory to such offences.

Section 3 – Disqualification from tender process and exclusion from future contract

If the Bidder(s) / Contractor(s), before award or during execution has committed a transgression through a violation of Section 2 of integrity pact, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s) / Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealing".

Section 4 – Compensation for Damages

i. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3 of integrity pact, the principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit / Bid Security and other actual damages due to consequential delay.

ii. If the Principal has terminated the contract according to Section 3 of integrity pact, or if the principal is entitled to terminate the contract according to Section 3 of integrity pact, the principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

i. The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

ii. If the Bidder makes incorrect statement on this subject, he can be disqualified from the 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 / Contractors / Subcontractors

i. The Bidder(s) / Contractor(s) undertakes(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

ii. The principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

iii. The principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the principal has substantive suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

i. The principal appoints competent and credible Independent External Monitor for this 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 agreement.

ii. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders / Contractors as confidential. He reports to the STPI.

iii. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the principal including that provided by the Contractor. The Contractor 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. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality.

iv. The principal will provide to the Monitor enough information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

v. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management 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.

vi. The Monitor will submit a written report to the STPI within 8 to 10 weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.

vii. If the Monitor has reported to the STPI substantiated suspicion of an offence under relevant IPC/PC Act, and the STPI 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.

viii. The word **'Monitor'** would include both singular and plural.

Section 9 – Pact Duration

i. Pact becomes effective on signing & submission with bid by bidder.

ii. For the successful bidder, the Integrity Pact ends after 10 months from last payment made to the successful bidder.

iii. For unsuccessful bidders, valid for six months after award of contract.

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 STPI.

Section 10 – Other provisions

i. This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e., New Delhi.

ii. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

iii. If the Contractor is a partnership, this agreement must be signed by all partner members and in case of a Company, by an authorized representative.

iv. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to co me to an agreement to their original intentions.

v. 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 Principal) (For & On behalf of Bidder/Contractor)

Name of HOD and Dept. (Office Seal)
(Office Seal)

Place _______________

Date _______________

Witness 1:

(Name & Address) _________________________
____

Witness 2:

(Name & Address) _________________________
____

Annexure O: MSP's Parent/Group Company Authorization

<<To be printed on Parent/Group Letterhead and signed by Authorized Signatory>>

Date:

To
Tender Division,
Software Technology Parks of India, B, office block
1st floor, Plate, 1, East Kidwai Nagar
New Delhi -110023
Tel: 011-24628081/ 24346600
Email – cloudrfp@stpi.in

Ref: RFP for Selection of MSP for setting up and Managing Government Community Cloud (GCC) & Hybrid Cloud in Revenue Share Model

Dear Sir,

It is certified that we, M/S ……………… <Registered name of Parent Company/Group Company and its communication address>, having permanent office in India at…………….. <Office Address >, do hereby authorize M/s…………………… <Registered name of the Bidder (MSP) and its communication address> to participate and submit a bid against the RFP as referred above.

<Registered name of Parent Company/Group Company> does hereby undertake to guarantee any shortfall of performance by < bidder name> in successful delivery of services and abide by all terms and condition of this RFP as defined for bidder.

Yours faithfully,

Name & Designation
of the Authorized Signatory of the CSP
Date:
Place:
Note:

- This is applicable in case of MSP is using Parent Company/Group credential for the bidding purpose
- Proof of relationship between bidder and parent entity needs to be submitted duly signed by authorised signatory.

Annexure P: Documents Checklist

#	Required document	Reference document/ page no. in the bid
1.	Earnest Money Deposit (EMD)	
2.	Certificate of incorporation	
3.	Corporate Identification Number (CIN)	
4.	GST registration certificate	
5.	Permanent Account Number (PAN)	
6.	Copy of IT returns	
7.	Office registration certificate or tax receipt	
8.	Copy of audited profit and loss account and balance sheet of the last three financial years and Certificate from statutory auditor/CA quantifying the average annual revenue from Data Centre/Cloud related services.	
9.	For Net worth: Statutory Auditor Certificate with Registration Number and Seal	
10.	For external projects, Copy of work orders along with completion certificate (for successful implementation) from the Client.	
11.	For external projects, in case of non-Disclosure agreement (NDA) with Client only provide an undertaking in this regard must be provided by the Statutory Auditor.	
12.	For Internal projects, an undertaking in this regard must be provided by the bidder on its company letter head duly signed and stamped from authorized signatory. Undertaking should clearly specify the scope of work, project start, Go- Live date, current status and total project value including taxes.	
13.	For NoC Experience, Self-Certificate along with the name, address, contact person, contact no., and email address of the customer.	
14.	For SoC Experience, Self-Certificate along with the name, address, contact person, contact no., and email address of the customer.	

#	**Required document**	**Reference document/ page no. in the bid**
15.	For Manpower, Certificate from statutory auditor/ Signing Authority (HR head) / copy of certificates of certified employees (MSP)	
16.	Copy of Valid Certificate 1. ISO 9001:2015 2. ISO 20000 3. ISO 27001	
17.	As per MSP Pre-Qualification Criteria, for Mandatory Undertaking provide Self-certification by the authorized signatory duly signed and stamped on the company letterhead	
18.	As per MSP Pre-Qualification Criteria, for IT Act provide Self-declaration from the Authorized signatory of the bidder on their letterhead	
19.	As per Pre-Qualification Criteria for CSP, for Turnover provide Copy of audited profit and loss account and balance sheet of the three financial years and Certificate from the statutory auditor/CA quantifying the average annual turnover	
20.	CSP Presence and Services, copy of i. Certificate of incorporation ii. GST registration certificate iii. PAN	
21.	ISO Certifications: Valid Copy of these certificates (a)ISO 20000 (b)ISO 27001 (c)ISO 27701	
22.	As per Pre-Qualification Criteria for CSP for Data Centre Facility a. Valid Copy of uptime/TIA 942 certificate b. Confirmation from the bidder on Tier-III/Rated 3 standards c. Declaration Form	
23.	For Accreditations, Copy of SOC1, SOC2 and SOC3 Certificate / Reports	
24.	For Financially Backed SLA a. CSP Self-Declaration from the authorized signatory.	

#	**Required document**	**Reference document/ page no. in the bid**
	b.URL of the public portal where in SLAs of services offered on Public Cloud are furnished.	
25.	For Operations provide References of work orders/Purchase order/ Completion Certificate with name, address, contact person, and contact No, email address Or Self-Declaration Refer Form Annexure-D	
26.	For Blacklist, CSP Self-Declaration from the authorized signatory	
27.	For List of Services, CSP Self-Declaration and proof from CSP's online portal	
28.	For MeitY Empanelment, Self-declaration from the Authorized signatory of the CSP on their letterhead along with the URL of the public portal of MeitY where in details of empanelment containing CSP name is visible	
29.	Proposal document a. Approach and Methodology b. Business Model c. Proposed Technical Solution	
30.	Bidder's experience and setting up operating and managing cloud operations Provide Copies of relevant work orders or Client Certificate / contract documentation depicting the said experience credentials must be submitted for 1, 2 & 3, (Ref. Technical Evaluation Parameters, Section B)	
31.	Technical Presentation and Demonstration 1. Technical Presentation 2. Response to Q & A session with Evaluation Committee 3. Demonstration Plan: Bidder shall demonstrate/submit documentary proof for POC (Proof of Capability) as part of technical evaluation	
	Annexures	
32.	CSP Authorization Format (CAF)	
33.	Annexure A: Bid Covering Letter	
34.	Annexure B: Format for Earnest Money Deposit	

#	**Required document**	**Reference document/ page no. in the bid**
35.	Annexure C: Performance Bank Guarantee	
36.	Annexure E: Compliance sheet for qualification	
37.	Annexure H: Technical Specification	
38.	Annexure I: Demonstration Plan	
39.	Annexure J: Template for Commercial Bid	
40.	Annexure K: Template for the CV of proposed manpower	
41.	Annexure L: General information of the Bidder	
42.	Annexure O: MSP’s Parent/Group Company Authorization	