

No. 10(26)/2024-NICSI

**National Informatics Centre Services Inc.
(NICSI)**

**company under
National Informatics Centre, Ministry of Electronics & Information
Technology,
Government of India**

**REQUEST FOR EMPANELMENT
MANAGED SERVICE PROVIDERS (MSPs) - RATE
FOR PROVISIONING OF CLOUD SERVICES**

RFE No. NICSI/CLOUD SERVICE PROVIDERS- RATES/2025/04



1st Floor, NBCC Tower
15, Bhikaji Cama Place, New Delhi: - 110066
Tel: 011-22900525/534/35, Email – tender-nicsi@nic.in

DISCLAIMER

1. The sole objective of this document (the Request for Empanelment or the RFE) is to solicit Techno commercial offers from interested parties for taking part in the empanelment process leading to empanelment of service provider(s) for the scope of work as mentioned in this document. While this document has been prepared in good faith, no representation or warranty, express or implied, is or will be made, and no responsibility or liability will be accepted by NICSI or any of their employees, advisors or agents as to or in relation to the accuracy or completeness of this document and any liability thereof is hereby expressly disclaimed. Each Bidder should conduct their own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFE Document and wherever necessary, obtain independent advice from appropriate sources.
2. Interested Parties may carry out their own study/analysis/investigation as required before submitting their Techno commercial proposals.
3. This document does not constitute an offer or invitation, or solicitation of an offer, nor does this document or anything contained herein, shall form a basis of any agreement or commitment whatsoever.
4. NICSI Representatives, its employees and advisors make no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of the RFE Document.
5. Some of the activities listed to be carried out by NICSI subsequent to the receipt of the responses are indicative only. NICSI has the right to continue with these activities, modify the sequence of activities, add new activities or remove some of the activities, as dictated by the best interests of NICSI.
6. It is advised through this REF that materialistic misrepresentation of facts shall be dealt with seriously and may lead to barring of the bidder from all NICSI tenders/RFEs for a period of minimum 3 (three) years. Bidders are requested to share information which is true and based on some tangible proofs.
7. The information contained in this RFE is subject to update, expansion, revision and amendment prior to the last day of submission of the Bids at the sole discretion of NICSI. In case any major revisions to this RFE are made by NICSI within seven days preceding the last date of submission of the Bids, NICSI may, at its discretion, provide reasonable additional time to the Bidders to respond to this RFE. Neither NICSI nor any of its officers, employees, advisors nor consultants undertakes to provide any Bidder with access to any additional information or to update the information in this RFE.
8. The Bidders shall bear all 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 NICSI or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and NICSI shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

TABLE OF CONTENTS

Table of Contents

1. FACTSHEET	6
2. ABBREVIATIONS	7
3. DEFINITIONS	9
4. INVITATION TO BID	11
5. INTRODUCTION.....	12
5.1. ABOUT NICS I.....	12
5.2. BACKGROUND AND OBJECTIVE	13
6. SCOPE OF WORK	14
6.1 Role of the Managed Service Provider (MSP)	15
6.2 Role of the Cloud Service Provider (CSP)	18
6.3 List of Services.....	19
6.4 Detailed Scope of Work.....	22
6.5 RACI (Responsible, Accountable, Consulted, Informed) MATRIX	27
7. INSTRUCTIONS TO BIDDERS	29
7.1. Availability of RFE	29
7.2. Pre-Bid Queries & Clarifications	29
7.3. Duration of Appointment.....	30
7.4. Amendment of REF Documents	30
7.5. Language of Bid.....	31
7.6. Bid Cost and Validity.....	31
7.7. Tier Category for Bidders	31
7.8. Earnest Money Deposit (EMD).....	32
7.9. Basic Compliance Requirement of Cloud Services	32
7.10 NICS I Cloud Pricing Platform	34
7.11 Eligibility of Bidding Entities.....	34
7.12 Nomination and Management of Authorized MSPs.....	34
7.13 Bid Submission	35
7.14 Other Instructions	36
8. EVALUATION PROCESS.....	38
8.1. Pre-Qualification Evaluation	38
8.2. Technical Evaluation	38

8.3.	Financial Evaluation	39
9.	<i>EMPANELMENT</i>	41
9.1.	Signing of Contract	41
9.2.	Price Revision	42
9.3.	Security Deposit for Empanelment.....	43
9.4.	Performance Bank Guarantee (PBG).....	44
10.	<i>PLACEMENTS OF WORKORDERS</i>	45
11.	<i>ADDITION OF NEW SERVICES</i>	46
12.	<i>PAYMENT TERMS & SCHEDULE</i>	47
13.	<i>SERVICE LEVEL REQUIREMENTS (SLAs)</i>	48
13.1	SLAs (Service Legal Agreement)	48
13.2	Support/Helpdesk Tool and SLA Management Tool	51
13.3	Incident Severity Levels & Critical Services	51
13.4	Contract Compliance and Resolution Mechanism	52
13.5	Monthly Service Level Availability	52
14	<i>PENALTY</i>	67
15	<i>EXIT MANAGEMENT</i>	68
15.1	Exit Management Plan	69
15.2	Exit Management Services	69
16	<i>SPECIAL TERMS & CONDITIONS</i>	70
16.1.	General Conditions.....	70
16.1.	Manpower/Resource Related Conditions	71
16.2.	Empanelment Exclusivity and Usage Authorization	72
16.3.	Cloud Agnostic Services	72
16.4.	Indemnification & Limitation of Liability	73
16.5.	Labour Laws.....	74
16.6.	Termination of Contract	75
16.7.	Force Majeure	76
16.8.	Fraud and Corrupt Practices	77
16.9.	Governing Law and Jurisdiction	78
16.10.	Arbitration	78
16.11.	Conciliation	79
16.12.	Applicable Law	79
16.13.	Non-Solicitation	79
16.14.	Confidentiality	79

16.15.	Intellectual Property Rights (IPR).....	80
17.	ANNEXURES	82
1.1.	Pre-Qualification Evaluation for CSP	83
1.2.	Pre-Qualification Evaluation for MSP	91
	ANNEXURE 2: Technical Evaluation Criteria	100
2.1.	Technical Evaluation Criteria for CSPs:.....	100
	ANNEXURE 3: COVERING LETTER	111
	ANNEXURE 4: Format for Earnest Money Deposit (EMD)	113
	ANNEXURE 5: Format for Bid Securing Declaration	114
	ANNEXURE 6: Format for Power of Attorney / Bidder's Authorization Certificate	115
	ANNEXURE 7: Form for Submission of Pre-qualification Information	116
7.1.	Compliance Sheet for CSPs Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)	116
7.2.	Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)	118
7.3.	Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)	120
7.4.	Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)	122
7.5.	Compliance Sheet for MSPs - Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)	125
7.6.	Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)	126
7.7.	Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)	129
7.8.	Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)	132
	ANNEXURE 8: Form for Submission of Technical Compliance	137
8.1.	Compliance Sheet for CSPs – Technical Qualification Criteria (Tier-1 for Basic Cloud Services)	137
8.2.	Compliance Sheet for CSPs – Technical Qualification Criteria (Tier-2 for Intermediate Cloud Services)	138
8.3.	Compliance Sheet for CSPs - Technical Qualification Criteria (Tier-3 for Advanced Cloud Services)	143
	ANNEXURE 9: Indicative Bill of Quantities (BoQ).....	149
9.1.	BoQ for Tier-1 (Basic Cloud Services)	149
9.2.	BoQ for Tier-2 (Intermediate Cloud Services)	153
9.3.	BoQ for Tier-3 (Advanced Cloud Services)	159
	ANNEXURE 10: Undertaking from HR demonstrating its Organization Strength.....	168
	ANNEXURE 11: Format for Project Experience	169
	ANNEXURE 12: Self-declaration for Non-Blacklisting.....	170
	ANNEXURE 13: Undertaking on Absence of Conflict of Interest.....	171
	ANNEXURE 14: Commercial Cover Letter.....	172
	ANNEXURE 15: Abridged Financial Bid	174
15.1	GROSS TOTAL VALUE (GTV)	174
	ANNEXURE 16: Detailed Financial Bid	175
16.1	Financial Bid Format for Tier-1 (Basic Cloud Services)	175

16.2	Financial Bid Format for Tier-2 (Intermediate Cloud Services)	180
16.3	Financial Bid Format for Tier-3 (Advanced Cloud Services).....	187
16.4	Financial Bid Format for Resources	200
ANNEXURE 17: Undertaking to Maintain KYC of Customers as per CERT-In Guidelines		202
ANNEXURE 18: Undertaking by the CSP		204
ANNEXURE 19: Undertaking by the MSP		205
ANNEXURE 20: Format for Non-Disclosure Agreement (NDA).....		206
ANNEXURE 21: Auditor’s Certificate for Positive Net worth		207
ANNEXURE 22: Auditor’s Certificate for Avg. Annual Turnover (CSP).....		208
ANNEXURE 23: Auditor’s Certificate for Avg. Annual Turnover (MSP)		209

1. FACTSHEET

RFE No.	NICSI/CLOUD SERVICE PROVIDERS- RATES/2025/04
Name of Organization	National Informatics Centre Services Inc. (NICSI)
RFE Type	Open RFE
RFE Category	Services
Type of Contract	Empanelment
Service Category	MSP/CSP for Provisioning of Cloud Services
Selection Method	As per RFE
Availability of Bid Document	e-procurement portal at https://eprocure.gov.in
Cost of the Bid Document (RFE fee)	Nil
Contract (Empanelment) Period	Total contract period is for Five (05) years from the date of award of contract. The contract may be extended by a period of 2 years or more (post completion of 5 years).
Service provider Panel	<ul style="list-style-type: none"> ➤ Tier 1: Basic ➤ Tier 2: Intermediate ➤ Tier 3: Advanced
Earnest Money Deposit (EMD)	<p>Bidders shall submit, along with their Proposals, EMD / Bid Securing Declaration as per ANNEXURE-4 / ANNEXURE-5 (To be submitted on Non-Judicial Stamp paper of minimum Rs. 100)</p> <p>Bidders EMD – BG/eBG from any scheduled commercial bank for Tier-1, Tier 2 and Tier 3: INR 10,00,00,000/- (Rupees Ten Crore) valid for 180 days from the last date of bid submission. Will need to be extended, if bid validity is extended.</p>
Bid Validity	Proposals shall remain valid for 180 days from the last date of bid submission
Proposal Language	English
Proposal Currency	INR (Indian Rupees)
Date of Publication	30.05.2025 at e-procurement portal site https://etenders.gov.in/eprocure/app
Sub-Contracting / Consortium	Not Allowed
Last Date for Pre-Bid Queries Submission	06.06.2025 at 15:00 Hours
Pre-Bid Meeting Date & Venue	09.06.2025 at 15:00 Hours (NICSI HQ)
Last Date & Time for Bid Submission	23.06.2025 at 15:00 Hours
Opening of Technical Bids	24.06.2025 at 15:30 Hours
Opening of Financial Bids	Technically qualified bidders to be notified later
Number of Packets	Two Packets Online bid submission as under: 1.Packet-1 Technical Bid (EMD/Bid Security Declaration/Eligibility & Technical Bid)

	2.Packet-2 Financial Bids (Abridged & Detailed Financial)
Re-Bid Submission	Yes (Before last date of bid submission)
Bid Withdrawal	Yes (Before last date of bid submission)
Address for Communication	Tender Division NICS National Informatics Centre Services Inc. 1stFloor, 15 NBCC Tower, Bhikaji Cama Place, New Delhi-110066 Email: tender-nicsi@nic.in , Phone: 011-22900525/34/35

Note:

The above dates, time and venue may be altered by the Purchaser at its sole discretion after giving prior notice to the Bidders. Some of the information provided in the above FACTSHEET is further elaborated in the subsequent sections of this RFE and the information provided in the FACTSHEET and subsequent sections of this RFE are to be read in conjunction and are to be interpreted harmoniously.

2. ABBREVIATIONS

The following table elaborates the terminologies used in this RFE and the reference to/ definition of these terminologies.

S. No	Acronym	Reference to/Definition
1.	BOM	Bill of Material
2.	BC	Business Continuity
3.	BOQ	Bill of Quantity same as BOM
4.	Cr	Crores
5.	DC	Data Centre
6.	DR	Disaster Recovery
7.	DSC	Digital Signature Certificates
8.	EMD	Earnest Money Deposit
9.	ES	Enterprise Solution
10.	FAT	Final Acceptance Test
11.	GoI	Government of India
12.	GST	Goods and Service Tax
13.	HoD	Head of Department
14.	HQ	Head Quarters
15.	HW	Hardware
16.	INR	Indian Rupee

17.	ISP	Internet Service Provider
18.	ISO	International Organization for Standardization
19.	MeitY	Ministry of Electronics and Information Technology
20.	NIC	National Informatics Centre
21.	NICSI	National Informatics Centre Services Incorporated
22.	OEM	Original Equipment Manufacturer as defined in IFB
23.	O&M	Operations and Maintenance
24.	OPEX	Operational Expenditure
25.	PAYG	Pay As You Go
26.	PBG	Performance Bank Guarantee
27.	PDC	Primary Data Centre
28.	PSU	Public Sector Undertaking
29.	QA/QC	Quality Assurance / Quality Control
30.	QOS	Quality of Services
31.	RDC	Remote Data Centre
32.	RFE	Request for Empanelment
33.	RMS	Root Mean Square
34.	SDC	Secondary Data Centre
35.	SLA	Service Level Agreement
36.	SOW	Scope of Work
37.	STQC	Standardisation Testing and Quality Certification
38.	SW	Software
39.	TAC	Technical Assistance Centre
40.	TCV	Total Contract Value
41.	TPA	Third Party Agency
42.	UI	User Interface
43.	VAPT	Vulnerability Assessment and Penetration Testing

3. DEFINITIONS

In this document, the following terms shall have respective meanings as indicated:

"NICSI" shall mean National Informatics Centre Services Incorporated, New Delhi. The term NICSI includes successors and assigns of NICSI.

"NIC" shall mean National Informatics Centre, New Delhi.

"Client/User department" shall mean the department/organisation for which the order is being placed.

"e-Governance" ICT (Information and Communication Technology) based projects in government sector

"RFE" shall mean Request for Empanelment or Bidding Document including the written clarifications issued by NICSI in respect of the RFE.

"Authorized Representative/Agency" shall mean any person/agency authorized by NICSI.

"Contract" shall mean the Work Order placed by NICSI on successful Bidder and all attached exhibits and documents referred to therein and all terms and conditions thereof together with any subsequent modifications thereto.

"Financial Year" (FY) period from 1st of April till 31st of March of subsequent year.

"Specifications" shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Bidding Documents.

"Bidder/Agency/Service Provider" means the firm offering the solution(s), services and/or materials required in the RFE. The word Bidder when used in the pre award period shall be synonymous with Bidder, and when used after intimation of Successful Bidder shall mean the Successful Bidder, also called "Agency", on whom NICSI places Work Order for Delivery of services.

"Party" shall mean NICSI or Bidder individually and "Parties" shall mean NICSI and Bidder collectively.

"Services" means requirements defined in this document including all additional services associated thereto to be delivered by the Bidder.

"SME" means subject matter expert is an individual with a deep understanding of a particular job, process, department, function, technology, machine, material or type of equipment.

"Proposal/Bid" means the Bidder's reply or submission in response to this RFE.

“Service Category” refers to a defined group of related services that are bundled based on their functional nature, technical scope, or delivery objectives. Each service category outlines a specific area of work—such as Compute as managed service, Storage as a Managed Service etc.

“Tier Category” refers to the classification of service providers based on their capabilities, experience, and scale of operations, divided into Tier-1, Tier-2, and Tier-3.

“Empanelment Rate” refers to the approved rate or discount finalized during the bidder empanelment process for a specific service category. It serves as the baseline pricing that the empanelled service provider agrees to offer for delivering defined services during the contract period.

“Material Breach” means a breach by the selected bidder of any of its obligations under this Agreement which has or is likely to have an Adverse Effect on the Project which such Party shall have failed to cure.

“CSP” means the Particular cloud services provider whose services the bidder is bidding and has submitted the letter of authorization from the CSP.

“MSP” Managed service provider, the empanelled bidder who will provide cloud services, if CSP bids under this RFE has to fulfil all the condition mentioned in this RFE for MSP.

“CSP Native Market Place” means a centralized platform where cloud services from CSP marketplace are available for purchase by customers, with single point support & resolution from CSP, SLA compliance from CSP, and single console billing from the CSP.

“DR Centre/Secondary Data Centre” refers to the Disaster Recovery Data Centre.

“Business Hours” shall refer to the period from 09:00 AM to 06:00 PM (Indian Standard Time - IST), Monday through Saturday, excluding gazetted public holidays as notified by the Government of India.

4. INVITATION TO BID

NICSI (National Informatics Centre Services Inc.) invites proposals or bids in response to this Request for Empanelment (RFE) from qualified bidders for the "Rate Contract Empanelment of Managed Service Providers (MSPs) for Provisioning of Cloud Services" for various projects of NICSI and its clients.

Interested bidders are advised to study this RFE carefully before submitting their proposals in response to the RFE. Submission of proposal in response to this RFE shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions, and implications.

Interested parties can access and download the REF document, which includes detailed terms and conditions, free of cost from CPP portal (<https://eprocure.gov.in>). Bids must be submitted in accordance with the procedures outlined in the RFE document.

Any subsequent corrigendum/clarifications shall also be made available on CPP Portal. Proposals must be received not later than time and date mentioned in the FACTSHEET. Proposals that are received after the deadline WILL NOT be considered in this empanelment process.

Bidders shall be selected under procedures described in this RFE.

Bidders may send their pre-bid queries in the format and time as specified in this RFE.

5. INTRODUCTION

5.1. ABOUT NICSI

National Informatics Centre Services Inc. (NICSI) was established in 1995 as a Section-25 (now Section 8 under the Companies Act, 2013) company under the National Informatics Centre, Ministry of Electronics & Information Technology, Government of India. NICSI provides and procures IT solutions for a variety of e-governance projects undertaken by NIC, MeitY, and various Government Organizations (including Public Sector Undertakings).

With a turnover exceeding **Rs. 2,500 crores (FY-2023-24)**, NICSI is a leading IT company with a strong government-facing focus. Over the past 25 years, NICSI has successfully executed over **20,000 projects** across India and other developing nations. It has delivered state-of-the-art, cost-effective solutions tailored to the growing ICT needs of its clients. These solutions are sourced from high-quality bidders, empanelled with NICSI/GeM, and the procurement processes are fully compliant with the GFR rules of the Government of India.

As the demand for cloud-based services continues to rise, particularly in the government sector, NICSI has expanded its focus towards providing **cloud computing solutions** to meet the evolving needs of its clients. The NICSI Cloud Business has experienced significant growth, driven by the increasing adoption of **cloud services** by government departments and Public Sector Undertakings (PSUs) for hosting mission-critical applications, data storage, and disaster recovery. The demand for scalable and secure cloud services is accelerating across central and state government organizations, as well as for specific public sector initiatives.

NICSI's role in cloud services involves providing a wide array of products and services, including **private and hybrid cloud solutions, data centre services, and cloud infrastructure**. The growing demand for these services is propelled by the increasing need for **digital transformation** within government agencies, where cloud adoption offers benefits such as enhanced efficiency, cost savings, and improved service delivery.

Objectives:

- **To foster economic, scientific, technological, social, and cultural development in India** by promoting the utilization of Information Technology, Computer Communication Networks, Informatics, and related infrastructure, including **NICNET** (the NIC's Computer-Communication Network).
- **To expand the services, technologies, and expertise developed by NIC**, thereby increasing the revenue-earning capacity of NICSI.
- **To develop and promote value-added IT services** over the basic infrastructure developed by NIC, such as **cloud-based applications, software development, and IT consulting services**.

In pursuit of these goals, NICSI has been a trusted partner, successfully executing more than 850 projects, providing a range of cloud services and IT solutions to organizations in the Central

Government, State Governments, and PSUs. These include cloud-based hardware, systems software, application software, cloud-based networking services, and IT implementation support.

NICSI's **cloud business** continues to see exponential growth, reflecting the increasing demand for scalable and secure digital infrastructures to support **e-governance initiatives, data storage, and cloud-enabled services** across various government sectors.

Through these services, NICSI plays a critical role in enabling effective e-Governance and fostering digital transformation across government organizations. For more information, please visit <https://nicsi.com/>.

5.2. BACKGROUND AND OBJECTIVE

In today's era of digital transformation, the strategic adoption of cloud services is essential for enhancing operational efficiency and ensuring robust, scalable IT infrastructures across government agencies. Recognizing this critical need, NICSI has initiated the empanelment process for Managed Service Providers (MSPs) for the provisioning of cloud services. This initiative aims to establish a pre-qualified panel of industry-leading providers who can deliver state-of-the-art, secure, and compliant cloud solutions tailored to the unique requirements of public sector organizations.

By streamlining the procurement process and promoting transparent, competitive practices, this empanelment framework not only accelerates access to high-quality cloud services but also aligns with the broader digital transformation goals of the government. The selected MSPs/CSPs will be rigorously evaluated on technical expertise, security standards, and regulatory compliance, ensuring that government departments can confidently leverage innovative cloud solutions that drive efficiency, resilience, and improved service delivery.

Government agencies are increasingly reliant on cloud-based infrastructures to enhance service delivery, ensure data security, and support mission-critical operations. Currently, the capacity of National Data Centres (NDCs) is fully utilized, and the demand for cloud services has significantly increased. The demand is projected in terms of megawatts (MW), reflecting the substantial computing power and energy consumption required to support critical e-governance applications. Several government ministries and departments are actively utilizing cloud services, including: Ministry of Agriculture & Farmers Welfare, Ministry of Justice, Ministry of Home Affairs, Ministry of Consumers Affairs, and many more.

However, the growing demand for such services necessitates a streamlined procurement process that guarantees compliance with stringent technical, security, and regulatory standards. By empanelling qualified MSPs, NICSI aims to ensure that agencies have prompt access to innovative cloud services that align with the strategic objectives of digital transformation and modern governance.

However, it is important to note that the empanelment of these bidders will be strictly time-bound and project-specific. This arrangement is designed to meet the operational needs of NICSI and User departments without creating any form of employment obligation. The bidders' contributions

will be focused on delivering defined outputs within a specified timeframe, ensuring flexibility and scalability in addressing project requirements. The empanelled bidders will be required to provide services across India.

Objectives:

The empanelment of Managed Service Providers by NICSI is driven by the following key objectives:

- **Streamlining Procurement:** To onboard MSPs/CSPs to reduce the administrative burden on the government for bid process management. Establish a robust and transparent framework that simplifies the procurement process, enabling timely access to cloud services without compromising on quality or compliance.
- **Uniform Pricing Benefits:** To ensure equal discounts for small-volume projects.
- **Access to Specialized Expertise:** Cloud technology requires specialized knowledge, which many ministries and departments may lack. This empanelment will enable them to engage MSPs/CSPs conveniently as needed.
- **Enhanced Service Quality:** Ensure that only providers meeting the highest standards of technical expertise, security, and regulatory compliance are selected, thereby delivering reliable and high-performance cloud solutions.
- **Compliance Assurance:** Align cloud service engagements with established government financial and procurement guidelines, ensuring adherence to all relevant policies and standards.
- **Innovation and Agility:** Foster an environment that promotes technological innovation and operational agility, empowering government agencies to leverage modern cloud capabilities in a rapidly evolving digital landscape.
- **Cost-Effectiveness:** Facilitate competitive practices among providers, ensuring that government agencies benefit from cost-effective solutions that deliver maximum value.
- **Support for Digital Transformation:** Enable government entities to achieve their digital transformation goals by providing access to state-of-the-art cloud services that enhance data security, operational efficiency, and service delivery.

Overall, this empanelment initiative is designed to build a strong foundation for the strategic adoption of cloud technologies across government agencies, ensuring that they are well-equipped to meet current and future digital challenges.

6. SCOPE OF WORK

Introduction

With the growing demand for cloud services across government entities, NICSI aims to establish a standardized framework to streamline procurement, ensure cost-effective service delivery, and enhance efficiency for government and PSU applications. This initiative is designed to simplify the procurement process by providing standardized pricing for managed cloud services, ensuring cost

efficiency, service reliability, and seamless delivery of high-quality cloud infrastructure and managed services to various ministries and government departments, facilitated through NICSI.

The rate contract will be structured based on the quality and scope of services offered by each MSP/CSP and the L1 rate will be determined through a competitive bidding process, guaranteeing the most cost-effective solution for the government without compromising on service quality.

This framework is intended to facilitate the seamless procurement and integration of cloud services for government projects while fostering competition and innovation. Additionally, the empanelment process will incorporate quality-driven selection criteria, compliance with national security and data localization regulations, and a structured operational support model to enhance service delivery.

The empanelment will cover a wide range of cloud services, from basic infrastructure to advanced cloud solutions, ensuring scalability, security, and operational excellence across ministries and departments. All MSPs/CSPs shall have to follow all the guidelines/policies/security compliance as and when issued by Government of India.

6.1 Role of the Managed Service Provider (MSP)

The Managed Service Provider (MSP) plays a critical role in ensuring the seamless deployment, operation, and management of cloud services. The key responsibilities of the MSP shall include but not limited to:

- a. Cloud Service Management:
 - i. Responsible for the design, deployment, and management of cloud services.
 - ii. Ensure optimal performance, security and scalability of cloud-based solutions.
- b. Application Integration & Infrastructure Support:
 - i. Oversee end-to-end application integration, ensuring seamless connectivity between cloud-hosted applications and existing government systems.
 - ii. Provide and manage the necessary supporting infrastructure to meet project requirements.
- c. SLA Monitoring & Compliance:
 - i. Develop and maintain a dashboard for SLA tracking, offering real-time insights into performance, uptime, resource utilization, and incident resolution.
 - ii. Ensure compliance with Service Level Agreements (SLAs) as specified in the empanelment terms and project agreements.
- d. Security & Regulatory Compliance:
 - i. Implement and manage security protocols, access controls, and data protection measures in alignment with government regulations and MeitY guidelines.
 - ii. Ensure adherence to national security policies, data localization requirements, and compliance standards.
- e. Certified Resources & Skilled Workforce:
 - i. Provide CSP-certified professionals with expertise in cloud management, security, and application deployment.
 - ii. Ensure continuous skill enhancement and resource availability as per project needs.
- f. Usage Reporting and Billing Management:
 - i. Track system usage and usage reports.
 - ii. Monitoring, managing, and administering the monetary terms of SLAs and other billing related aspects.

- iii. Provide the relevant reports including real time as well as past data/information/reports for the department to validate the billing and SLA related penalties. The reports shall consist of (not limited to) of:
 - Summary of resolved unresolved and escalated issues / complaints.
 - Logs of backup and restoration undertaken reports.
 - Component wise Virtual machines availability and resource utilization reports.
 - Consolidated SLA / Non- conformance reports.
 - g. Workloads Migration:
 - i. Inventory of existing applications, infrastructure, and data, Map dependencies, identify critical systems, and categorize applications for migration readiness.
 - ii. Ensure successful migration of Scoped applications as per best practices of Migration planning and Strategy
 - h. Provision of Third-Party Services
 - i. The MSP may engage or provide third-party services for the execution of specific components of the project, subject to prior written approval from NICSI.
 - ii. The MSP shall remain solely accountable for the performance, compliance, and delivery of services by any approved third-party entity, in accordance with the terms and conditions of this RFE/contract.
 - i. Operational Support & Customization:
 - i. Offer ongoing operational support, including troubleshooting, performance optimization, and periodic system upgrades.
 - ii. Accommodate any additional terms and conditions specified by the user department, considering the unique requirements of each project.

6.1.1 Migration Planning and Strategy

Cloud migration involves moving IT assets, applications, DBs and data from on-premises data centres to a public cloud environment. This transformation leverages cloud benefits like scalability, agility, cost efficiency, and enhanced security. A successful migration follows these core phases, which are the scope of bidder in the RFP and ensure the best practices are followed at every phase of the migration. The Customers/departments application, Data & workloads may vary depending on the existing/running environments but fundamental principles of migration will remain as described below:

- a. Phase 1: Assessment & Strategy: Understand current state and define migration:**
 - i. Discovery & Inventory: Catalog IT assets, configurations, and dependencies.
 - ii. Application Assessment: Evaluate cloud readiness, complexity, and criticality.
 - iii. Strategy Selection: Choose migration approach such as Rehost, Re-platform, Refactor etc. as per Requirements
- b. Phase 2: Planning & Design: Develop a detailed, actionable migration roadmap:**
 - i. Cloud Architecture: Design target cloud environment (VPCs, security, IAM, compute, storage, DBs) per best practices.
 - ii. Migration Plan: Create phased roadmap, prioritize workloads, and define waves and timelines.
 - iii. Data Migration: Plan data movement, ensuring integrity, security, and minimal downtime.
 - iv. Security & Compliance: Design cloud security controls, access policies, and ensure regulatory adherence.

- v. Cost Management: Plan budgeting, tagging, and optimization strategies.
 - vi. Governance: Define policies for resource provisioning, usage, and change management.
 - vii. Skills & Training: Assess gaps; plan team upskilling.
 - viii. Backup & DR: Establish backup and disaster recovery.
- c. Phase 3: Migration Execution: Execute workload transfer to the cloud:**
- i. Environment Prep: Provision and configure cloud infrastructure.
 - ii. Pilot Migrations: Conduct small-scale migrations to validate processes.
 - iii. Data Migration: Execute data transfer, ensuring consistency.
 - iv. Application Migration: Migrate applications using chosen strategies.
 - v. Continuous Testing: Perform ongoing functional, performance, and security tests in the consultation with application team
 - vi. Rollback Plan: Establish a clear rollback strategy if required
- d. Phase 4: Validation & Cutover: Verify functionality and transition production traffic:**
- i. Testing: Conduct functional, performance, security, and User Acceptance Testing (UAT) in the consultation with application team
 - ii. Performance Benchmarking: Compare cloud vs. on-premises performance.
 - iii. Security Validation: Verify security controls effectiveness.
 - iv. Pre-Cutover Checks: Confirm readiness, connectivity, and data sync.
 - v. Cutover Execution: Redirect production traffic (during maintenance window).
 - vi. Post-Cutover Monitoring: Monitor stability, performance, and errors.
- e. Phase 5: Optimization & Operations: Maximize cloud benefits and ensure ongoing excellence:**
- i. Performance Optimization: Fine-tune cloud resources for optimal performance.
 - ii. Cost Optimization (FinOps): Continuously monitor spending; identify cost reduction areas.
 - iii. Security & Compliance: Ongoing monitoring, vulnerability management, and compliance.
 - iv. Automate Operations: Implement Infrastructure as Code (IaC), CI/CD, and cloud-native automation.
 - v. Monitoring & Alerting: Set up robust monitoring, logging, and alerts.
 - vi. Governance Refinement: Continuously refine cloud governance policies.

6.1.2 Service Delivery Timelines for MSPs: The MSPs will have clear responsibilities for the deployment, operation, and maintenance of cloud infrastructure. For each cloud service, MSPs must meet the following timelines:

- a. Cloud Infrastructure Provisioning: The MSP must provision cloud infrastructure within 10 business days from the date of the final approval for a project.
- b. Ongoing Operations: The MSP must ensure that the cloud infrastructure and applications are fully operational and optimized within 15 business days of deployment.
- c. Performance Monitoring: The MSP is required to submit monthly performance reports including metrics such as uptime, resource utilization, and incident resolution times, ensuring that all service levels are consistently met. Service Level Agreements (SLAs) will specify that uptime must meet or exceed 99.5% on a monthly basis.

6.2 Role of the Cloud Service Provider (CSP)

Cloud Service Providers (CSPs) shall be responsible for delivering cloud infrastructure services, ensuring seamless and secure operations for government projects. Their key responsibilities include:

- a. Cloud Infrastructure Provisioning:
 - i. Provide compute, storage, and networking resources as per project requirements.
 - ii. Ensure high availability, scalability, and reliability of cloud services.
- b. Security & Compliance:
 - i. Implement robust security measures, including data encryption, access controls, and threat detection.
 - ii. Ensure compliance with MeitY guidelines, data localization policies, and national cybersecurity regulations.
- c. Service Level Agreements (SLAs) & Performance Monitoring:
 - i. Adhere to predefined SLAs, ensuring a minimum uptime of 99.5% or as specified in the contract.
 - ii. Provide real-time monitoring and reporting on cloud resource utilization and system performance.
- d. Scalability & Optimization:
 - i. Offer flexible and cost-efficient scaling of cloud resources to accommodate varying workloads.
 - ii. Optimize infrastructure to enhance performance, efficiency, cost-effectiveness and cost-optimization on monthly basis.
- e. Collaboration with MSPs:
 - i. Work with authorized MSPs for service deployment and management.
 - ii. Ensure that MSPs comply with all contractual obligations and service standards.
- f. Resource Utilization Monitoring and Optimization:
 - i. If a user department utilizes less than 30% of provisioned services over a month, the Cloud Service Provider (CSP) will issue an alert indicating low resource utilization and recommend deprovisioning of surplus resources.
 - ii. If the user department fail to act upon this alert, the CSP will escalate the recommendation to Level 2 (L2).
 - iii. If L2 does not respond, this is responsibility of CSP to optimize services to a threshold of 50% utilization.
 - iv. Similarly, if a User department utilizes more than 20% of the provisional resources/services over a month, alert must be issued for over utilization and to avoid heavy billings.
- g. Third-Party Service Arrangements:
 - i. If a user department requires third-party services, the CSP may facilitate these arrangements.
 - ii. The Third-Party Service Provider (TPA) will be responsible for providing support related to these services.
- h. Application Performance Management (APM) Services:
 - i. The CSP will offer Application Performance Management/ Monitoring (APM) services on a chargeable basis, tailored to the specific requirements of the user department.
- i. Virtual Private Cloud (VPC) and Dedicated Infrastructure:
 - i. VPC and dedicated infrastructure services, including physical separation, will be included in the service offering.
- j. Disaster Recovery (DR) Replication Charges:

- i. The user department is responsible for the charges associated with standard DR replication services.
- ii. Any discrepancies, such as mismatches in storage components or delays in replication attributable to the CSP, will be borne by the CSP.

6.3 List of Services

NICSI shall evaluate bidders applying under various categories (Tier-1, Tier-2, and Tier-3) based on their capability to deliver the below listed services, but not limited to, in the respective Tier category.

6.3 (A): Tier-1 – BASIC CLOUD SERVICES

TIER 1: BASIC CLOUD SERVICES	
A. Compute as Managed Service	
Production Grade Virtual Machine <ul style="list-style-type: none"> • RED HAT Enterprise Linux • Open-Source Linux - Debian, CentOS, Ubuntu • Windows Standard and Datacentre edition O/S with Cloud Based O/S Licenses 	
B. Storage as a Managed Service - Object, File and Block Storage	
<ul style="list-style-type: none"> • Object Storage - Hot Tier • Enterprise-grade network file system (NFS) • Managed Storage- SSD 	
C. CSP/MSP Managed DB - Managed services	
<ul style="list-style-type: none"> • Managed Database services (Non burstable x86 Intel architecture - Production Grade) 	
D. Other Managed /additional services/Network /Back up / Security	
<ul style="list-style-type: none"> • Cloud Management and Monitoring • Site to Site VPN - Managed Service • Managed Application Load balancer (L7) • Managed TCP Load balancer (L3/L4) • NAT Gateway • Backup as Service • Domain Name System (DNS) • Data transfer /Egress over the Internet • Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud • Public IP • Managed DDoS Protection and WAF • Network Firewall – NGFW 	

6.3 (B): Tier-2 – INTERMEDIATE CLOUD SERVICES

TIER 2: INTERMEDIATE CLOUD SERVICES	
A. Compute as Managed Service	
Production Grade Virtual Machine <ul style="list-style-type: none"> • RED HAT Enterprise Linux • Open-Source Linux - Debian, CentOS, Ubuntu • Windows Standard and Datacentre edition O/S with Cloud Based O/S Licenses 	
B. Storage as a Managed Service - Object, File and Block Storage	

<ul style="list-style-type: none"> Object Storage - Hot Tier Enterprise-grade network file system (NFS) Managed Storage- SSD Archive Storage
C. CSP/MSP Managed DB - Managed services
<ul style="list-style-type: none"> Managed Database services (Non burstable x86 Intel architecture - Production Grade)
D. Other Managed /additional services/Network /Back up / Security
<ul style="list-style-type: none"> Cloud Management and Monitoring Site to Site VPN - Managed Service Managed Application Load balancer (L7) Managed TCP Load balancer (L3/L4) NAT Gateway Backup as Service Domain Name System (DNS) Data transfer /Egress over the Internet Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud Public IP Managed DDoS Protection and WAF Network Firewall - NGFW Container Registry Managed Kubernetes (Production Grade, SLA Backed) DevOps and Application Monitoring Cloud Posture Management
E. CSP Content Delivery Network (CDN)
<ul style="list-style-type: none"> Managed Content Delivery Network (CDN)
F. GPU As Service
<ul style="list-style-type: none"> Production Grade Virtual Machine with GPU (Define TFlops)

6.3 (C): Tier-3 – ADVANCED CLOUD SERVICES

TIER 3: ADVANCED CLOUD SERVICES
A. Compute as Managed Service
Production Grade Virtual Machine <ul style="list-style-type: none"> RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL Open-Source Linux - Debian CentOS, Ubuntu Windows Standard and Datacentre edition O/S with Cloud Based O/S Licenses & native billing
B. Storage as a Managed Service - Object, File and Block Storage
<ul style="list-style-type: none"> Object Storage - Hot Tier Cloud Native Enterprise-grade network file system (NFS) Single SSD redundant volume from Storage tier which support Sub-millisecond latency performance for Mission Critical Web, Apps, Databases Archive Storage with milliseconds restore tier
C. CSP/MSP Managed DB - Managed services
<ul style="list-style-type: none"> CSP Native Managed Database services (Non burstable x86 Intel architecture - Production Grade) CSP Native Redis Cluster as Service - Production Grade supporting Sharding Production Grade CSP Native Managed Non- Relational Database (NoSQL) as Managed Services

D. Other Managed /additional services/Network /Back up / Security
<ul style="list-style-type: none"> • Cloud Management and Monitoring • Site to Site VPN - CSP Managed Service • CSP Natively Managed Application Load balancer (L7) • CSP Natively Managed TCP Load balancer (L3/L4) • NAT Gateway • Backup as Service • Domain Name System (DNS) • Data transfer /Egress over the Internet • Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud • Public IP • Managed DDoS Protection and WAF • Network Firewall - Cloud Native NGFW • CSP native Container Registry • Managed Kubernetes (Production Grade, SLA Backed) • DevOps and Application Monitoring • Cloud Posture Management • Messaging services
E. CSP Native Content Delivery Network (CDN)
<ul style="list-style-type: none"> • Managed CSP Native Content Delivery Network (CDN)
F. GPU As Service
<ul style="list-style-type: none"> • Production Grade Virtual Machine with GPU (Define TFlops)
G. CSP Native AI/ML & Data Warehouse Platform
<ul style="list-style-type: none"> • ML Notebook • ML Training • ML Inference • Fully Managed Data Warehouse • Managed ETL as a Service • Data Visualization /BI Service
H. Generative AI As Service
<ul style="list-style-type: none"> • GenAI - Multimodal models • Translation • Enterprise Chat bot

Note:

- To qualify for empanelment, it is mandatory for CSPs to have Public Pricing available for all service categories and also shall provide the Public Pricing for their offered service categories through NICSI Pricing Platform.
- All CSPs shall ensure seamless integration of its public pricing platform with the NICSI Pricing Platform through a secure API only.
- Performance and availability metrics must be integrated into the rate contracts to ensure service quality, reliability, and compliance with predefined Service Level Agreements (SLAs).
- Given that purchasers may have requirements spanning multiple departments, projects, and state/central government initiatives, cloud services must support integration, adoption, and migration across various environments, including Production, Staging, Testing, or any other environment as per project needs.
- For migrating existing Production services, the approach should follow either Lift-and-Shift or minimal modifications as required by the project.

- f. It is the responsibility of the empanelled MSPs/CSPs to ensure the delivery of all services as outlined in the Scope of Work and Bill of Material (BoM), in accordance with the project's Work Order.
- g. MSPs may collaborate with MeitY empanelled CSPs only for service delivery. However, the MSPs shall remain fully responsible for the overall operation, performance, and compliance of the CSPs. The MSP must ensure that the CSP adheres to all contractual obligations, service level agreements (SLAs), and regulatory requirements as specified in the RFE. Any failure on the part of the CSP will be deemed the responsibility of the MSP, and necessary corrective actions must be taken by the MSP to ensure seamless service delivery.

6.4 Detailed Scope of Work

The empanelled MSPs/CSPs shall perform the activities as per the scope of work given below, but not limited to:

6.4.1 General Responsibilities

- a. The MSP shall be responsible for proposed cloud "Secure Landing zone, Optimized resources, Scalable services, designing and provisioning" of required cloud infrastructure for hosting applications.
- b. The MSP/CSP shall examine the application landscape through a comprehensive gap analysis that needs to be hosted on cloud infrastructure. This activity may enable the MSP/CSP to gauge the Application workload criticality & complexity before provisioning managed hosting services and the Network Connectivity required for it.
- c. The MSP/CSP shall be responsible for deployment, operation and maintenance of the applications on the Cloud infrastructure as per the requirement of the project.
- d. The MSP/CSP shall ensure that the cloud platform shall have the capability to scale, without any performance disruption. There shall be sufficient buffer capacity available for resources like compute, storage, network, security, etc. to take care of anticipated growth.
- e. The underlying infrastructure shall be robust enough to ensure maximum uptime and "round-the-clock" availability of applications services as per the defined SLA. The MSP/CSP must maintain an uptime of 99.95% availability of services and platform on monthly basis.
- f. The MSP shall provide inter-operability support with regard to available APIs, data portability etc. for the User department to utilize in case of change of Cloud service provider, migration back to on premise infrastructure, burst to a different Cloud service provider for a short duration or availing backup or DR services from a different Cloud Service provider.
- g. The MSP shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the defined SLA's.
- h. The MSP shall maintain adequate bench strength to meet contingencies, ensure measures for BCP and meet the SLA requirement as per this RFE.
- i. MSP shall ensure for the support (Proactive & Reactive) should be offered through a combination of channels viz. telephonic, remote, or onsite support (if situation warrants), at the same SLAs as stated in the response to RFE.
- j. The MSP/CSP should submit a well-defined disaster recovery (Active-Active, Active-Passive, or any other) and business continuity plan including processes, policies, and procedures related to preparing for recovery or continuation of Services, based on the mutual discussion with the User department.

- k. The MSP shall submit undertaking/confirmation from respective empanelled CSP whose services are offered to NICSI/User department. They shall be responsible for the privacy and security safeguards.
- l. The CSP should support BYOL from different OEMs and any technical support for various aspects of the project.
- m. The MSP/CSP shall bring in their Professional Consulting Support and Technical Support.
- n. All the data shall be hosted by the CSP within the geographical boundary of India.
- o. The MSP/CSP shall support Audit of usage of Cloud services by NICSI/ User department whenever required.
- p. The MSP/CSP shall report any Security incident to NICSI/ User department immediately on occurrence and shall initiate actions as per the defined standards. The MSP/CSP shall also recommend NICSI/ User department on further actions.
- q. In case of any breach, loss, leakage or theft of data because of the action/omission of the MSP/CSP, the MSP/CSP will be penalized as per the provisions of the Acts of India in addition to the provisions of the RFE.
- r. No copy of data or any information shall be retained/exported/backed-up after the end of Contract/work order. The data stored shall not be used for any purposes by the MSP/CSP.
- s. The MSP and the CSP are jointly and severally responsible for the Data Security. System Integrator, Platform developer and the CSP shall comply with Acts, Rules, directions, guidelines, advisories (both current and future) of Government of India on Data handling and Data Storage. NICSI/ User department reserves the right to penalize and seek remedy under various Acts including Information Technology Act 2000, Indian Contract Act, 1872 and Consumer Protection Act, 2019 in addition to the provisions in the Contract agreement.
- t. In the event of non-compliance with any of the above clauses (q, r, and s), including but not limited to data breaches, unauthorized retention or misuse of data, or violation of applicable legal or regulatory provisions, NICSI reserves the right to initiate debarment proceedings against the MSP/CSP. This may include temporary or permanent disqualification from current and future empanelment, contracts, or tenders floated by NICSI or any other affiliated government entities. Debarment shall be in addition to any legal, financial, or contractual penalties imposed under applicable laws and the terms of the contract.
- u. In addition to the listed scope of work, the bidder may also provide services that may evolve over time during the empanelment period.

6.4.2 Cloud Infrastructure Management

- a. The MSP/CSP shall ensure for provisioning required compute infrastructure (Servers/Virtual Machines), storage and network as per the project requirements.
- b. The MSP/CSP shall be responsible for deployment, operation and maintenance of the applications on the Cloud infrastructure as per the requirement of the project.
- c. The MSP/CSP will be responsible for provisioning of requisite network infrastructure and connectivity to ensure accessibility of the cloud servers / virtual machines as per defined SLAs.
- d. The MSP/CSP will be responsible for operating and maintaining the cloud infrastructure 24*7, resolving all incidents, and meet performance parameters as defined in the SLA Section and best practices followed by the industry.

- e. The MSP/CSP shall ensure to scale up (or scale down) the resource requirements (compute, memory, storage, bandwidth etc.) based on the growth in the user compute load / data load / bandwidth load (during peak and non-peak periods / year-on-year increase) to support the scalability and performance requirements.
- f. At least 30% headroom for scaling up / scaling down should happen automatically. If beyond 50% then the MSP/CSP shall provide the necessary details including the sizing calculations, assumptions, current workloads and utilizations, expected growth / demand and any other.
- g. The MSP/CSP shall submit the infrastructure utilization 'usage matrix' as and when required.

6.4.3 Storage

- a. The CSP shall provide scalable, dynamic, and redundant storage with efficient storage tiering features and configurable life cycle management should be used for efficient data retention.
- b. The MSP/CSP shall provide the storage solution to meet IOPS requirements of frequent, infrequent & archival data storage for different workload.
- c. The MSP/CSP shall implement efficient data storage solutions that can handle increased volumes of data during peak periods without compromising on performance.
- d. The CSP shall support attaching of storage volume to multiple compute instances in R/W mode so that users can access and share a common data source.
- e. The CSP shall provide versioning, where multiple versions of an object can be kept in one object storage account. Versioning shall be protected against unintended overwrites and deletions.
- f. The MSP/CSP shall ensure that data shall be encrypted adequately in rest and as well as in-transit to maintain the integrity.
- g. The CSP shall support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
- h. The CSP shall support encryption using a Key Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.
- i. The stored data must support WORM functionality to ensure that the immutable copy of data is made available in case of an incident in alignment with data retention policies of NICSI/User department.
- j. The CSP shall be able to provide audit logs on storage account including details like the timestamp when the data access activities occurred (Using API etc.), Source of the activity, Target of the activity, Type of action and Type of response.

6.4.4 Backup Solution

- a. The backup service is to ensure that each of the cloud resources, workloads, and services is appropriately backed up and protected. The MSP/CSP shall be responsible for the provisioning and maintaining the backup in the cloud environment as per the below backup schedule timelines.

Backup Type	Data
Full backup	Weekly, Monthly, yearly

Incremental Backup	Daily
Retention	One Year
Archival	Yearly copy during complete project tenure. The final set must be handed over to the department on exit.

- b. The MSP shall provision with regular incremental and full backups with proper retention and testing mechanisms and shall adhere to the following restoration timelines or as agreed as per the terms and conditions with the User department:

#	Backup Type	Backup Frequency	Retention Period
1	Incremental	Daily	14 Days
2	Full	Weekly	45 Days
3	Full	Monthly	12 Months
4	Full	Yearly	5 Years

- c. The MSP/CSP shall provide testing and validation of backup and restore procedures.

#	Restoration Timelines	
1	Backup taken in last month	Once in a month
2	Backup taken in last Quarter	Once in a Quarter

- d. Backup of all system software configurations inclusive of customized source code, database configurations, events & audit log, device mapping & integration configuration, user configuration, and any other data stored on cloud shall be backed-up regularly and restore data to ensure complete recovery in case of any disruptions.
- e. The MSP/CSP shall ensure that data is stored in immutable backup with proper encryption and version enablement feature so that the data cannot be modified and deleted under any circumstances.
- f. The backups shall be a fully automated procedure requiring no manual intervention, shall be scheduled during non-peak hours and completion status reports shall be circulated to authorized persons through emails.
- g. Backup service shall allow to create customized backup schedules to meet business and regulatory backup requirements.

6.4.5 Data Governance and Security

- a. The cloud services provided by the empanelled MSPs/CSPs must adhere to a Zero Trust Security Architecture. This architecture ensures (but not limited to) that:
- All users are authenticated and authorized using multi-factor authentication (MFA) before accessing any cloud resources.
 - Internal and external network traffic is not trusted by default, and all requests must be validated at multiple levels before being allowed access to resources.
- b. The MSP/CSP shall provide and manage the adequate security solution for NICS/ User department which includes security at the perimeter (FW, IPS, VPN for secure remote access, DDOS, WAF), for authentication (PKI, IDAM, SSO, AD/LDAP, MFA, HSM/KMS, SSL certificate) and internal security measures (endpoint/VMs security, container security, Anti-APT etc.).

- c. The CSP/MSP shall provision below network security services to secure the overall System environment.
 - i. DDoS protection
 - ii. WAF functionality
 - iii. NGFW
 - iv. IPS
 - v. End-Point protection for VM/Containers
 - vi. Data Encryption at rest and in transit
 - vii. SSL off-loader
 - viii. Data protection
 - ix. SIEM and SOAR
 - x. Network Zoning/Micro-segmentation
 - xi. DNS Security
 - xii. Identity Access Management (IAM) and Privileged Access Management (PAM)
 - xiii. Others (If required)
- d. The MSP/CSP shall ensure that all applications, services, and systems developed, deployed, or managed under this engagement strictly adhere to the security best practices outlined in the latest OWASP Top 10 vulnerabilities list.
- e. The MSP/CSP shall always ensure continual compliance with Cloud security guidelines of MeitY/Cert-In/NIC/NICSI.
- f. All components and other system integrated with NICSI/User department should have defined mechanism/solution/tools to view and identify malicious user activities and potential security incidents through audit logs.
- g. The MSP/CSP shall provide cloud services that support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, login attempts, login failure, software installation attempts, security logs, and so on.
- h. The MSP/CSP shall ensure that the proposed firewall rules/policies can but are not limited to provide state-full inspection, filter packets based on protocol/source & destination address/source & destination ports, support for protection of common internet applications like mail, DNS, AAA, etc. and must prevent IP Spoofing, be able to filter malicious viz. Java Applets, ActiveX and perform Network Address Translation.
- i. The MSP shall ensure to provide and manage Layer 3 & Layer 7 protection to protect workloads against known and unknown threats, brute force attacks etc.
- j. The MSP/CSP shall implement robust encryption techniques and maintain appropriate key management to protect data while it is in transit and at rest.
- k. The MSP/CSP shall provision SSL certificates for the web servers that are being used to access the web applications.
- l. Antivirus and proxy server administrators shall ensure that up-to-date antivirus signatures and OS patches are available on the servers.
- m. The bidder shall ensure strict compliance with the guidelines issued by the Indian Computer Emergency Response Team (CERT-In), particularly with respect to the maintenance of Know Your Customer (KYC) information. The bidder shall be responsible for collecting, verifying, and maintaining accurate KYC details of all end-users/customers, including name, address, contact information, and valid proof of identity, as applicable.
- n. The bidder shall retain such information securely for a minimum period of **five (5) years** or as mandated under prevailing laws, from the date of cessation of the relationship with the

customer. The KYC data shall be made available to CERT-In or any authorized government agency upon lawful request. The bidder shall also ensure that such data is stored in a secure manner, protected against unauthorized access, and handled in compliance with applicable data protection and cybersecurity regulations.

6.4.6. Advanced Services

- a. The MSP/CSP will be responsible for delivering advanced cloud services, including AI-driven solutions, machine learning (ML) capabilities, and advanced data analytics tools.
- b. The MSP/CSP will offer support for cutting-edge technologies such as, native AI/ML frameworks, data warehouse platforms, and generative AI services for innovation and automation.
- c. The MSP/CSP will provide GPU-based cloud computing resources/environment for high-performance processing needs, facilitating scalable deep learning, AI model training, and data-intensive operations.
- d. The MSP/CSP will ensure seamless integration and management of intelligent chatbots and conversational AI platforms to enhance customer interaction and support.
- e. The MSP/CSP will provide advanced cloud services for data-driven decision-making, including robust data warehousing, ETL, and analytics platforms.

6.5 RACI (Responsible, Accountable, Consulted, Informed) MATRIX

The RACI matrix breaks down responsibilities across the key stakeholders. The identified stakeholders for this empanelment include the following:

- i. NICS
- ii. CSP
- iii. MSP
- iv. User departments/Ministries
- v. TPA (Third Party Providers)

The RACI matrix is not limited to and may be revised with the approval of NICS.

#	Activity / Deliverable	NICS	CSP/MSP	CSP/MSP	User Department
1	Cloud services/ Infrastructure Administration & Management				
1.1	End to end Management of Infrastructure resources	I	R, A	R	
1.2	Active monitoring and performance management of infrastructure resources	I	R, A	R	
1.3	Performance Monitoring and Reporting	I	R	R	C
1.4	Proactively notify Incidents on CSP infrastructure based on monitoring	I	R/A	R/A	I
1.5	Security and Compliance Implementation	I	R/A	R/A	C
1.6	Security event management & Remediating instances infected with malware.	I	R/A	R/A	I
1.7	Back-up, DR Drill, Disaster Recovery Replication & Management	I	R/A	R/A	C

1.8	Update Security services & Configuration	I	R/A	R/A	I
1.9	Optimization of Underutilized Resources	I	R/A	R/A	C
1.10	Third-Party Service Facilitation	I	R	R	C
1.11	APM & Monitoring Services Delivery	I	R/A	R/A	C
1.12	Compliance to Government Policies & Future Guidelines	A	R	R	I
1.13	Skill Certification and Availability of Experts	I	R	R	C
1.14	Monthly Reporting to NICSI	A	R	R	I
1.15	Issue Resolution & Escalation Management	A	R/A	R/A	C
1.16	Project-specific Customization & Tuning	I	R	R	C
2	Monitoring , Logging and Event Management				
2.1	Monitoring of IT Infrastructure resources utilization (i.e., Compute, Storage, network etc.)	I	R, A	R, A	I
2.2	OS Metrics Monitoring, logging, and event Management	I	R, A	R, A	I
2.3	Network Performance Monitoring	I	R, A	R, A	I
2.4	Provide a console to visualize the KPIs, metrics and logs	I	R, A	R, A	I
2.5	Creating the Informational/Warning/Critical notifications for defined threshold values	I	R, A	R, A	I
2.6	Comprehensive proactive monitoring and reporting of OS/Services/Warning/Critical alerts/events	I	R, A	R, A	I
2.7	Recording CSP infrastructure change logs	I	R, A	R, A	I
2.8	Investigating infrastructure Alerts for Incident notification	I	R, A	R, A	I
3	Service Level Agreements				
3.1	Availability of critical services	I	R, A	R, A	I
3.2	Infrastructure resources performance SLA	I	R, A	R, A	I
3.3	Incident and service request SLA	I	R, A	R, A	I
3.4	24*7 Support services SLA	I	R, A	R, A	I
4	Support Services				
4.1	24 x 7 Support	I	R	R, A	I
4.2	Define priority of issues and service request (i.e., Severity 1,2 and 3, etc.)	I	R	R, A	I
4.3	Incident management and reporting	I	R	R, A	I
4.4	Provide root cause analysis for critical issues	I	R	R, A	I

Legend:

- **R = Responsible** (Performs the work)
- **A = Accountable** (Owns the outcome, signs off on decisions)
- **C = Consulted** (Provides inputs based on expertise)
- **I = Informed** (Kept updated on progress or results)

7. INSTRUCTIONS TO BIDDERS

7.1. Availability of RFE

The RFE document is available on the e-procurement site at <https://eprocure.gov.in>.

Interested bidders who wish to participate in this REF may view and download the RFE document free of charge from the above-mentioned website.

Bidders are advised to thoroughly review all instructions, forms, terms, project requirements, and other relevant information provided in the RFE documents. Any failure to provide the required information or submission of a proposal that is not fully responsive to the RFE documents may result in the rejection of the proposal, at the bidder's risk.

REF Notice and detailed time schedule for this REF, will be accessible via the e-procurement site at <https://eprocure.gov.in>.

Bidders must comply with the timelines outlined in the **FACTSHEET** section. Bids submitted after the specified deadline will not be accepted.

The bidders participating first time on eProcurement portal will have to complete the Online Registration Process for the e-Tendering portal.

Bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFE documents. Failure to furnish all information required as mentioned in the RFE documents or submission of a proposal not substantially responsive to the RFE documents in every respect will be at the bidder's risk and may result in rejection of the proposal.

7.2. Pre-Bid Queries & Clarifications

For any clarifications regarding the RFE document or related matters, bidders may submit their queries to NICS I following the submission mode and timelines specified in the FACTSHEET. Pre-bid queries must include the name and details of the bidder submitting them. Queries submitted after the deadline indicated in the FACTSHEET will not be considered by NICS I.

NICS I reserves the right to issue responses, clarifications, or corrigenda as deemed necessary.

All queries must be submitted via email only, with the subject line formatted as follows:
“RFE for Rate Empanelment of” Pre-Bid Queries _<Bidder’s Name>

Pre-bid queries should be sent to the following email address: tender-nicsi@nic.in.

The queries should necessarily be submitted in **EXCEL** in the below format:

#	Name & Details of the Bidder	RFE Document Reference(s) (Section & Page No.)	Content of RFE requiring clarification	Point of Clarification

NICSI shall hold a pre bid meeting with the prospective bidders as per the schedule provided in the **FACTSHEET**. Queries received from the bidders regarding bidding conditions, bidding process, item specifications, evaluation criteria, etc., in writing, or over email (preferably in an excel file), **up till two (02) days prior to the pre bid meeting**, shall be addressed.

NICSI is not bound to clarify any query received after the day as described above. NICSI will review every query and on due consideration will issue corrigendum (if require). However, NICSI does not undertake to answer each individual query (ies). Bidders shall not assume that their unanswered queries have been accepted by NICSI.

7.3. Duration of Appointment

The initial term of the Empanelment will be for a period of **five (05) years**. This may be extended for up to an **additional two (2) years or more**, based on the Agency's performance as evaluated against the terms specified in this RFE and subject to successful MeitY empanelment, valid active certifications and no major security incident/default. Any renewal will adhere to the original Empanelment's terms and conditions, including financial terms. The decision of NICSI regarding renewal shall be final and binding on the Agency.

7.4. Amendment of REF Documents

- a) **Modification of REF Documents:** At any time prior to the deadline for bid submission, NICSI may, either on its own initiative or in response to a clarification request from a prospective bidder, amend or modify the REF document. Any such amendment will be communicated through a corrigendum on the CPP portal and will be binding on all prospective bidders. Bidders are required to consider the amendment and submit their proposals or quotations accordingly.
- b) **Extension of Bid Submission Deadline:** To allow prospective bidders adequate time to incorporate the amendment into their bids, NICSI may, at its discretion, extend the deadline for bid submission.
- c) **No Modifications or Withdrawals Post-Deadline:** Once the deadline for bid submission has passed, no bid may be modified. Additionally, no bid may be withdrawn between the submission deadline and the expiration of the bid validity period specified by the bidder. Withdrawal of a bid during this period may result in the execution of the EMD.

7.5. Language of Bid

The bid submitted by the bidder, along with all correspondence and documents exchanged between the bidder and NICS, must be in English. Supporting documents and printed materials provided by the bidder may be in another language, provided they are accompanied by an accurate English translation of the relevant sections. In case of any discrepancies between the original language and the translation, the English translation will prevail. Any information provided in a foreign language without an appropriate translation will be rejected.

7.6. Bid Cost and Validity

- a) The bidder shall bear all costs related to the preparation and submission of the bid. NICS will not be responsible or liable for any costs incurred, regardless of the outcome or conduct of the bidding process.
- b) All bids must remain valid for a minimum period of 180 days from the date of bid opening. The quoted rates must remain valid for the initial or extended duration of the empanelment period, starting from the date of empanelment, for placing the initial order.
- c) If required, NICS may request an extension of the bid validity period up to 90 more days. Bidders will have the right to refuse to extend the validity of bids beyond the said 90 days period and to withdraw the bids. The request and the responses thereto shall be made in writing or by email.

7.7. Tier Category for Bidders

Bidders may choose to apply for either TIER CATEGORIES: Tier-1, Tier-2 or Tier-3 based on the eligibility criteria specified in the RFE. The Bidders will be empanelled under (03) three categories:

- a) Tier 1 - Basic Cloud Services (e.g. IaaS including Marketplace) as per [Section-6.3 \(A\)](#).
- b) Tier 2 - Intermediate Cloud services (e.g. IaaS, PaaS & Other Cloud services including Marketplace) as per [Section-6.3 \(B\)](#).
- c) Tier 3 - Advanced Cloud Services (e.g. Including Basic, Intermediate & AI/ML, GenAI, APIs endpoints (all CSP Native Services Only)) as per [Section-6.3 \(C\)](#).

A bidder can submit a bid under only *one* tier category (either Tier-1 or Tier-2 or Tier-3). If a bidder submits proposals for more than one tier category, all the bids will be disqualified.

In the future, if a bidder seeks to move to a higher Tier category, NICS reserves the right to upgrade the bidder based on demonstrated capability and quality of services delivered. To qualify for the upgrade, the bidder must accept the empanelment rates or discounts applicable to the higher Tier category.

7.8. Earnest Money Deposit (EMD)

- a. Applicants shall submit an amount of **INR 10 Crore (Rupees Ten Crore only)**, as Earnest Money Deposit ("EMD").
- b. EMD must be in the form of a Bank Guarantee issued by any of the commercial banks in the format provided in the **ANNEXURE-4**.
- c. EMD in any other form will not be accepted.
- d. EMD shall be valid for a period of **180 days** from the last date of submission of the Application/Bid.
- e. Bank Details:
 - Beneficiary Name: National Informatics Centre Services Incorporated
 - Name of Bank: Union Bank of India
 - Branch: CGO Complex, Lodhi Road, New Delhi
 - IFSC CODE: UBIN0903710
 - A/c no. 520101263654539
- f. The bidders must submit the **original document of EMD**, in the form of Bank Guarantee (BG)/eBG form a scheduled commercial bank at NICSI HQ, Delhi within five days of closing time of Bid submission. NICSI accepts all standard BG format of the BG issuing bank.
- g. Copy of EMD document must be submitted along with Bid.
- h. If the EMD is not received within the stipulated time, the Purchaser reserves the right to immediately and summarily reject the proposal of the concerned bidder, without any further opportunity for correspondence.
- i. In case the bidder is seeking EMD exemption, the bidder must submit the valid supporting document for the relevant category with the bid. Under the Micro and Small Enterprise (MSEs) category, only Manufacturers for Goods and Services Providers for Services are eligible for exempted from submission of EMD. In lieu of EMD, the bidder must submit the "Bid Securing Declaration Form" in the format provided in **ANNEXURE-5: FORMAT FOR BID SECURING DECLARATION FORM**. The form should be uploaded to the CPP Portal as per the instructions in the bid submission section.
- j. The EMD of all unsuccessful applicants would be refunded by NICSI within three months of the applicant being notified by NICSI as being unsuccessful. The EMD of all the successful applicants would be refunded by NICSI within three months of the applicants acknowledging and accepting the Award of Empanelment by NICSI.
- k. No interest shall be payable by NICSI to the Applicant(s) on the EMD amount for the period of its currency.
- l. The application without adequate EMD, as mentioned above, will be liable for rejection without providing any further opportunity to the Applicant concerned.
- m. The applicant shall extend the validity of the EMD on request by NICSI.
- n. The EMD may be forfeited:
 - i. In case of a successful application, if the applicant fails to acknowledge and accept the Letter of Award of Empanelment from NICSI in accordance with terms and conditions.
 - ii. If the Applicant tries to influence the evaluation process.

7.9. Basic Compliance Requirement of Cloud Services

NICSI requires the empanelled Service Providers (MSPs/CSPs) to extend its services as per demand. The MSPs/CSPs should follow the below basic compliance requirement stated as below:

- a) The Cloud Service Offerings of CSP should be MeitY empanelled and STQC audited. The proposed Data Centre for hosting are empanelled by MeitY and should be clearly mentioned on the MeitY website (<https://meity.gov.in>).
- b) The CSP shall offer DR cloud services with their Data Centre location within India only. All the physical servers, storage, and other IT hardware from where cloud resources are provisioned for NICSI / User department must be within an Indian Data Centre only. MSP/CSP shall ensure that department data resides within India only.
- c) All monitoring, provisioning, should be within India and 100% isolated from other regions outside India.
- d) The empanelled MSPs through this RFE may be asked to provide the bouquet of services of their CSPs on the discovered discount rates on the public prices for current and future clients of NICSI. In this case, it is the responsibility of the empanelled MSP to ensure and meet all the Scope of Work as CSP as per this RFE.
- e) The CSPs shall comply with all security requirements applicable to the Bidder (MSP) as mandated by government bodies such as CERT-IN, throughout the empanelment period. The Bidder (MSP) must adhere to the security provisions outlined in the IT Act 2000, DPDP Act 2023, as well as any guidelines issued by government agencies from time to time, and the terms & conditions of the Provisional Empanelment of Bidders.
- f) The quantity and configuration of the service requested may vary for every project, and the bidder needs to make the provision for accommodating the same.
- g) CSP must be share their public pricing through API to NICSI pricing platform.
- h) The cloud service offerings of MSP/CSP shall always remain Empanelled / complied with the MeitY guidelines and standards. MSP shall be responsible for the costs associated with implementing, assessing, documenting and maintaining such Empanelment/ Compliances.
- i) To remain empanelled, MSPs/CSPs should ensure that the certifications remain valid throughout the empanelment period. In case, any certification is due for expiry, MSP/CSP shall renew the certification within a period of 60 days to avoid de-empanelment. If further time period is required for the renewal of certification, such extension should be subject to approval from competent authority.
- j) The bidder shall ensure full compliance with the scope of work and shall be responsible for providing all the services as specified in this RFE document. Partial or selective bidding for specific components or services shall not be accepted. Non-compliance or failure to deliver any of the listed services may lead to disqualification or termination of the contract, as deemed appropriate by the authority.
- k) The MSP/CSP shall ensure interoperability and data portability to facilitate seamless migration between cloud environments, and, upon contract termination or as directed by NICSI/User Department, must perform secure, complete, and verifiable deletion of all customer data—including backups and logs—from all systems. A data deletion certificate shall be submitted, and no data shall be retained thereafter, in compliance with applicable laws, including the IT Act, 2000, and DPDP Act.

7.10 NICSI Cloud Pricing Platform

- a) NICSI shall develop and deploy the NICSI pricing platform within a period of one year. This platform will serve as a centralized interface for monitoring and managing cloud service pricing from all empanelled agencies.
- b) Each empanelled agency shall ensure seamless integration of its public pricing platform with the NICSI Cloud Pricing Platform through a secure API. Any modifications to the public pricing by an empanelled agency will automatically trigger a notification on the NICSI platform.
- c) NICSI reserves the right to review all proposed price changes by CSPs. The acceptance or rejection of such modifications shall be at NICSI's sole discretion, ensuring compliance with procurement guidelines, budgetary considerations, and market competitiveness.

7.11 Eligibility of Bidding Entities

Only individual organizations (single bidding entities) are eligible to participate in the bidding process.

- a) Consortiums, joint ventures, or subsidiaries are not permitted to bid. The credentials of subsidiaries or affiliated companies will not be considered during the evaluation process.
- b) If a Managed Service Provider (MSP) is submitting a bid directly, it shall not authorize any of its partners, resellers, or affiliates to submit a separate bid for the same CSP solution. Any such duplicate or overlapping submissions will be deemed non-compliant and subject to immediate disqualification.
- c) Bidders must disclose any potential conflicts of interest, including affiliations with other bidding entities, that may impact the fairness of the selection process. NICSI reserves the right to reject bids if such conflicts are identified.
- d) The bidding entity must be a legally registered organization in India, compliant with all applicable laws, regulations, and financial obligations.
- e) The entity must not be blacklisted or debarred by any government department or regulatory authority at the time of bidding.
- f) One MSP shall be associated with a single CSP.
- g) All MSPs/CSPs must qualify the qualification and technical criteria as laid down in this RFE.
- h) For services offered in Tier-1, CSP can submit the bid with only one MSP.
- i) For services offered in Tier-2, one CSP can submit the bid with maximum two MSPs.
- j) For services offered in Tier-3, one CSP can submit the bid with maximum three MSPs.

7.12 Nomination and Management of Authorized MSPs

- a) CSPs may add/remove the Managed Service Providers (MSPs), as per the eligibility criteria of the RFE, post completion of one year of empanelment period.
- b) In case of removal of MSP, the same MSP will not be able to empanel with different CSP for a minimum period of 18 months from the date of their de-empanelment.

- c) Bidders may modify their panel of MSPs (add or remove) during the empanelment period. However, NICS I reserves the right to determine and enforce the maximum number of MSPs that may be associated with a single CSP at any given time.

7.13 Bid Submission

A two-stage bidding process will be followed for this RFE to finalize the selection of bidders. The bidders are required to submit the following bid documents on the CPP Portal:

Sl. No.	Bid Covers	Bid Submission
1	EMD / Bid Securing Declaration	To be uploaded on CPP Portal
2	Pre-qualification (PQ) & Technical bid	To be uploaded on CPP Portal
3	Financial bid including Abridged Financial Bid and Detailed Financial Bid	To be uploaded on CPP Portal

- a) **Technical Bid:** This should include all required documents related to Pre-qualification (PQ) as per [ANNEXURE-1](#) and Technical Evaluation criteria as per [ANNEXURE-2](#) including the bidder's eligibility, qualifications, and compliance with the technical specifications outlined in the REF document. No financial information should be included in this bid.
- All bids should submit the EMD / Bid Securing Declaration.
 - All the bid documents must be duly signed by the authorized signatory of the company and stamped with company seal.
 - It shall be the sole responsibility of the bidder to check (and double-check) the page number referencing made for supporting documents in the checklist indicated under Eligibility Compliance Sheet and Technical Compliance Sheet. No relevant information/document should be left, whether listed above or not.
 - Bidder must provide all documents mandated for bidder's profile, prequalification criteria and for technical evaluation criteria.
 - All pages of the bid being submitted must be sequentially numbered, stamped and signed by the authorized signatory.
 - Relevant referencing shall be done by the bidder, clearly indicating all page numbers where supporting documents are provided.
 - Technical Proposal should not contain commercials of the project, in either explicit or implicit form.
 - The Bidder may be required to give a presentation on their Proposal. NICS I will suggest the timing and venue of the presentation(s). 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 RFE.
 - Any technical proposal submitted on a conditional basis will be subject to rejection.
 - The document should have a Table of Contents indicating page no. where supporting document are placed.
- b) **Financial Bid:** This should contain the bidder's price quotation and detailed cost details as per [ANNEXURE-15](#) and [ANNEXURE-16](#).
- The Bidder must upload the BoQ as per the format provided on CPP portal. The bidder must adhere to terms and conditions and fill in the required details as required in BoQ.

- ii. The bidder must strictly follow the prescribed format as mentioned in the detailed Financial Bids.
- iii. The bidder shall quote only the GTV value in Abridged Financial Bid as derived from in Detailed Financial Bid, depending upon the Tier Category (Tier 1 or Tier 2 or Tier 3) for which bid is being quoted.
- iv. During financial opening, only the Abridged Financial Bid shall be opened for determining the L1 bidder based on the GTV value.
- v. Any other itemized financial details mentioned in the Abridged Financial Bid may lead to rejection of the bid.
- vi. All the bid documents should be duly signed by the authorized signatory of the company and stamped with company seal.

As the bid submission must be completed online, it is strongly advised that the bidder takes all necessary precautions to ensure a smooth process. This includes submitting the bid well in advance to avoid any last-minute issues, ensuring that file names and formats comply with the requirements for uploading the documents. NICS I will not consider any bids that are unable to be uploaded or are uploaded incorrectly on the portal, regardless of the reason.

7.14 Other Instructions

- a) This Request for Empanelment (RFE) is open for response by eligible Managed Service Providers (MSPs) and Cloud Service Providers (CSPs), who are empanelled with MeitY and meet the minimum eligibility criteria in the respective tier category.
- b) NICS I will not be responsible for any delay on the part of the bidder in submission of the bid.
- c) The bids submitted by Fax/E-mail etc. shall not be considered. No correspondence will be entertained on this matter.
- d) Conditional Bids shall not be accepted on any ground and shall be rejected straightway. (A bid is conditional when bidder submits its bid with his own conditions & stipulations extraneous to the terms and conditions specified in this REF). If any clarification is required, the same should be obtained before submission of the bids i.e. during pre-bid meeting.
- e) No bids will be accepted after the expiry of the deadline as stated in the Section1 - FACTSHEET.
- f) In case, the day of bid submission is declared Holiday by Govt. of India, the next working day will be treated as day for submission of bids. There will be no change in the timings.
- g) All pages of the bid being submitted must be signed by the authorized signatory, stamped and sequentially numbered by the bidder irrespective of the nature of content of the documents. Un-signed & un-stamped bid may be summarily rejected.
- h) Printed terms and conditions of the bidders will not be considered as forming part of their bid. In case any terms and conditions of the RFE document is/are not acceptable to the bidder or submitted any deviation, the bid shall be rejected summarily.
- i) Bids not submitted as per the specified format and nomenclature may be rejected.

- j) Ambiguous/Incomplete/Illegible bids may be out rightly rejected. Not quoted bids shall be consider as non-responsive and shall be rejected.
- k) Any alteration/ overwriting/ cutting in the bid should be duly countersigned else it will be out rightly rejected.
- l) Submission of the bid shall be considered as an acknowledgment that the bidder has thoroughly reviewed and understood all instructions, eligibility criteria, terms, and technical specifications outlined in the REF document. Bids that does not fully comply with the any given clause may be rejected. Failure to provide complete and accurate information or submitting a bid that is not substantially responsive to the REF document shall be at the bidder's own risk and may lead to disqualification.
- m) Bidders are advised to conduct their own independent assessments before submitting their bids.
- n) NICSI will not entertain any communications related to business or profit matters during the term of the contract.
- o) NICSI reserves the right to disqualify bids with quoted rates that are excessively 'low' or significantly deviate from prevailing market trends.
- p) The Bidder shall be responsible for providing both Cloud and Managed Services. All the costs (Hardware/ Software/ Services) including GST or other applicable taxes must be included in the quote as per the format prescribed in subsequent sections.
- q) REF process will be over after the issuance of empanelment letter(s) to the selected agency (ies).
- r) NICSI reserves the right to cancel this bidding process at any time prior to the execution of a formal written contract by or on behalf of the Purchaser.
- s) Bidders shall not use any part of their submission or any related clause as a means to market or promote their products or services.
- t) All CSPs shall provide their public links to the publicly available pricing as part of this bid submission. Subsequently, they shall integrate with the NICSI-developed platform via an API for real-time price updates.
- u) There is no minimum commitment of business in respect of the cloud services to be taken by the NICSI from the empanelled Service Provider either at present or in future.
- v) Any User Departments / Autonomous Agencies / Local Bodies under Central Government, State Governments, Educational Institutions may use any of the services of the proposed MSPs/CSPs from the empanelled bidders as per terms & conditions of NICSI.
- w) In the event that the terms *CSP* and *MSP* are found to be used interchangeably in certain contexts, the bidder is required to interpret such references contextually and in accordance with the roles, responsibilities, and scope of work defined for each. Where such interchangeable usage occurs, the bidder shall read and understand the intent accordingly, without attributing any difference in meaning unless explicitly stated.

For additional instructions, refer to the following Sections - Bid Evaluation, Technical Evaluation and Financial Bid Evaluation, etc.

8. EVALUATION PROCESS

NICSI will constitute a Technical Evaluation Committee (TEC) to evaluate the responses of the Bidders. The Committee shall evaluate the responses to the RFE and all supporting documents/documentary evidence. Bids will be assessed by adopting a three-stage evaluation process - Pre-Qualification Evaluation, Technical Evaluation, and Financial Evaluation.

NICSI will evaluate the responses of the Bidder and all the supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence, may lead to rejection.

No correspondence will be entertained outside the process of evaluation with NICSI.

NICSI reserves the right to reject any or all proposals. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFE.

In the event of the specified date of bid opening being declared a holiday for NICSI, the bids shall be opened at the appointed time and location on the next working day.

During evaluation of bids, the Committee may, at its discretion, seek clarifications or confirmations from the Bidder on the Technical & Financial Proposals. The request for clarification and the response shall be made in writing. If the response to the clarification is not received before the expiration of the deadline prescribed in the request, the Committee reserves the right to evaluate bids based on available documents which may also lead to rejection of the bid.

The decision of the Committee on the evaluation of responses to the RFE shall be final.

8.1. Pre-Qualification Evaluation

- The pre-qualification bid will be opened first and evaluated for compliance with the RFE requirements.
- Bidders must meet the mandatory pre-qualification criteria including experience, capacity, and capabilities to provide the services outlined under [ANNEXURE-1](#). The Bidder shall submit the information for prequalification in the form at [ANNEXURE-7](#).
- Any bidder failing to meet the mandatory pre-qualification criteria will be disqualified from further evaluation.
- Only bidders who successfully pass the pre-qualification stage will be eligible to proceed to the technical evaluation phase.

8.2. Technical Evaluation

The technical evaluation is aimed to assess the bidders' technical capabilities and their ability to meet the requirements specified in the REF documents. The evaluation will be based on the bidder's proposed solution, approach, methodology, experience, and overall technical merit.

- Bidders who meet the pre-qualification criteria will advance to the technical evaluation stage.

- The Technical Evaluation Committee will assess the technical proposals to verify compliance with the requirements as detailed under [ANNEXURE-2](#).
- All bids will be reviewed and scored based on the criteria mentioned above. Each criterion will be assigned a weightage, and the bidder's proposal will be evaluated and scored accordingly.
- The evaluation committee will review the Technical Bids of the short-listed Bidders to determine whether the technical bids are as per the requirements laid down.
- Any proposal that fails to meet the minimum technical threshold will be disqualified from further consideration.
- Each Technical Proposal will be assigned a technical score out of a maximum of a hundred (100) marks. Only the Bidders who get an overall technical score of seventy percent (70%) or more will qualify for selection. Failing to secure minimum marks shall lead to rejection of the bids and the Bidders.

8.3. Financial Evaluation

The financial bids of only those bidders will be opened who qualify the pre-qualifying and technical evaluation stage.

- a. On a designated day and time, the Abridged Financial Bids of only those Bidders satisfying all conditions of the eligibility criteria and have passed the Technical Evaluation Stage will be opened electronically in the presence of the representatives of the technically qualified bidders.
- b. The bidders in each tier category (Tier-1, Tier-2, Tier-3) with the lowest Gross Total Value (GTV) among all the quoted GTV in the Abridged Financial Bids will be selected as L1.
- c. The Detailed Financial Bid of only the L1 bidder for each tier category shall be opened and will be evaluated by a duly constituted Finance Evaluation Committee (FEC). However, based on the market trends, NICS I retains the right to negotiate this rate for future requirement.
- d. The bidder with the Second Lowest GTV among the Abridged Financial Bids in each tier category, will be the L2 bidder and will then be asked to match all the line item-wise price of L1, in order to be placed on the panel (within a time-frame prescribed by NICS I). If L2 does not agree, L3, L4 & so on...will be asked to match the line item-wise price of L-1. Thus, by way of successive opportunity a panel of bidders will be formed.
- e. If none of L2, L3, L4..... agree to match the L1 rates then L1 shall be the sole bidder on the panel. The decision of NICS I arrived at, as per above will be final for empanelment and no representation of any kind shall be entertained.
- f. Once the price match with empanelled rate is completed for each line item of different service categories by remaining bidders of respective Tier category, FEC will calculate the discount percentage in each service category.
- g. The empanelment for each service category shall be determined based on the weighted average of the percentage discounts or rates quoted across all line items within that particular service category. This approach ensures a balanced evaluation that reflects the overall pricing strategy rather than focusing on individual line items.

For example, in a service category for Tier-1 which includes multiple components—each with different cost weights—and different discounts, by L1 bidders. FEC will calculate the discount percentage as - empanelled rate / list price x 100%. The final empanelment discount for that service category will be calculated by applying the respective weights to the quoted percentages for each component.

In the scenario below, the list price is Rs.100 for line item “VM - 2 vCPU, 4GB RAM” and the lowest price quoted by different bidders in Tier-1 i.e. empanelled rate is Rs.80. Accordingly, the calculated discount is 20%. Similarly, overall discount for the service category i.e., “Compute as Managed Service (Tier-1)” will be weighted discount of 39%.

S. No	Service Name / Type of Service	Configuration /Description of Service	Specifications of required Service	Unit of Measure ment	List Price (Rs.)	Offered Price by L1 (Rs.)	Calculated Discount (%)*
A. Compute as Managed Service (Tier-1)							
1	Production Grade Virtual Machine	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Monthly / 730	100	80	20%
2			VM - 2 vCPU, 8GB RAM	Monthly / 730	200	120	40%
3			VM - 2 vCPU, 16GB RAM	Monthly / 730	400	220	45%
4			VM - 4 vCPU, 8GB RAM	Monthly / 730	800	400	50%
Discount in Service Category							39%

***Note: the calculated discount will be different for each line item.**

- h. In case, any bidder does not match the least price of the line item of the category, the bidder will not be empanelled.
- i. The final decision regarding price matching, re-evaluation, or bidder selection will rest with NICS and the Financial Evaluation Committee (FEC), ensuring transparency, competitiveness, and value for money.
- j. If NICS considers necessary, revised Financial Bids could be called from the eligible Bidders, before opening the original financial bids for recommending final empanelment.
- k. In the event of revised financial bids being called the revised bids should not be higher than the original bids, otherwise the bid shall be rejected.
- l. Quoting incredibly low or high value of items with a view to subverting the REF process shall be rejected straight away and execution of EMD/Bid Securing Declaration of such bidders.
- m. If there is a mismatch between values quoted in figures and words, the value quoted in words shall prevail.
- n. A Financial Evaluation Committee (FEC) would scrutinize the commercial bids. Bids found lacking in strict compliance to the commercial bid format shall be rejected straightaway.
- o. Arithmetical error will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price with quantity/weightage, the unit price shall prevail, and the total price shall be corrected. If the

bidder does not accept the correction of the errors, its bid will be rejected and EMD / Bid Securing Declaration will be executed. If there is a discrepancy between words and figures, the amount in words will prevail.

- p. NICS I reserves the right to use this REF to service NICS I/ User department's needs.
- q. The rates quoted should be as per industry standards for the prescribed experience. The bids in which the bidder quote NIL charges/considerations, such bid will be treated as unresponsive and will not be considered.
- r. In case the quoted prices involve components in foreign currency, the bidder shall explicitly mention the applicable **spot exchange rate** (as published by a recognized financial institution or central bank) used for conversion into Indian Rupees (INR) as on the date of submission of the bid. The quoted INR value shall be binding and no claims for exchange rate variation shall be entertained post submission.
- s. Bids of those bidders whose Financial Bid have a deviation beyond 30% (thirty Percent) on either side from the Average financial bid of all the technically qualified bidders would be liable for disqualification.
- t. The Financial Evaluation Committee (FEC) retains the right to enforce the deviation percentage clause mentioned above. Additionally, it reserves the authority to review and modify the deviation percentage, as specified in the Financial Bid Evaluation clause, considering prevailing market conditions, industry standards, and other relevant factors.

9. EMPANELMENT

9.1. Signing of Contract

- a) The NICS I would issue the letter of intent (LoI) to the successful bidders who meet the technical requirements and agree to the discovered L1 rates of the services they offer. Successful bidders should accept and sign the LoI within 15 days of issuance.
- b) The successful bidder would submit the operational readiness and third-party audit certification to NICS I. The TEC would review the operational readiness report and audit report and approve the successful bidder. NICS I will issue the Letter of Award (LoA) confirming the empanelment and operational readiness.
- c) On written communication from NICS I for having qualified for empanelment the bidder shall sign the contract (letter of empanelment) within 7 days of such communication. Failing which the offer shall be treated as withdrawn and execution of EMD/Bid Securing Declaration.
- d) NICS I would widely publish the list of empanelled bidders that are authorised, along with the prices for use by NICS I or any of the User departments.
- e) Empanelment will be initially for a **period of five years**, extendable for another **two years or more** solely at the discretion of NICS I on same terms and conditions or additional mutually agreeable conditions.
- f) NICS I will have a panel of bidder in three different tiers as defined under the Section-FACTSHEET.

- g) The empanelment can be used by NICSI or any User Ministry/department.
- h) The incidental expenses of execution of agreement/contract shall be borne by the empanelled bidder.
- i) After empanelment, selection procedure for issuance of Work Order / Purchase Order will be at the sole discretion of NICSI/User department. The Bidder will provide services as per NICSI/User Department's requirements.
- j) Escalation Matrix for Problem solving: The Empanelled agency should provide an escalation matrix for problem resolution to the user by providing the Names, Designations, Contact Number(s) and Email IDs of the persons to be contacted. The Empanelled agency should also provide website URL for such purpose.
- k) Empanelled agencies must honour all REF conditions and adherence to all aspect of fair-trade practices in executing the purchase orders placed by NICSI on behalf of its clients. Failing this, NICSI may execute of EMD/Bid Securing Declaration and stop further participation of such agency (ies) for a period of three years in NICSI tendering process.
- l) In the event, an Empanelled agency or the concerned division of the agency is taken over /bought over by another company, all the obligations and execution responsibilities under the agreement with NICSI, should be passed on for compliance by the new company in the negotiation for their transfer.
- m) During the empanelment, NICSI may ask the agency to submit the supporting documents which may be required to ensure that the REF terms and conditions are fulfilled.
- n) The agency should not assign or sublet the empanelment or any part of it to any other agency in any form. Any such attempt shall result in termination of empanelment and forfeiture of the security deposit, revocation of bank guarantees (including the ones submitted for other work orders).
- o) NICSI may, at any time, terminate the empanelment by giving written notice to the Empanelled agency without any compensation, if the Empanelled agency becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to NICSI.
- p) Reasons for rejecting a RFE/bid will be disclosed to a bidder only where enquiries are made.
- q) The empanelment will continue beyond one year, subject to the CSP/MSP meeting the terms and conditions and fulfilling the qualification criteria of the RFE.
- r) NICSI shall have sole discretion to onboard (rolling in) of new Cloud Service Providers (CSPs) or the exit (rolling out) of existing empanelled CSPs. Their respective MSP shall ensure full compliance with NICSI's directions and provide necessary support to facilitate a smooth and non-disruptive transition during such changes without any additional cost.

9.2. Price Revision

- a) The price revision process shall be conducted periodically— preferably every 12 months— or as deemed necessary by NICSI, based on prevailing industry trends, cost structures, and service benchmarks.

- b) No upward revision of prices will be permitted.
- c) No revision of prices will be permitted during the **first year** of empanelment. Post the first year, empanelled MSPs/CSPs may propose a price change **once in twelve months**.
- d) The agency shall notify NICSI regarding any price changes published on their official public websites minimum 90 days in advance.
- e) NICSI reserves the right to verify and validate the proposed changes before granting approval.
- f) The acceptance or rejection of such price modifications shall be at NICSI's sole discretion, ensuring adherence to procurement guidelines, budgetary constraints, and market competitiveness.
- g) Any price revision must align with prevailing market rates and must not adversely impact the procurement process.
- h) NICSI may conduct market analysis or benchmarking to assess the validity of the proposed price modifications.
- i) NICSI's decision on price revision requests shall be final and binding on all empanelled MSPs/CSPs.
- j) Any deviation from the approved rates without prior consent will result in the rejection of invoices and may lead to the termination of the empanelment agreement.
- k) If any new services/product are introduced by the empanelled agency in the service categories where bidder's discount are already empanelled, then the same discount shall be applicable to the new service/product of a respective category. Refer example at [Section \(8.3\) \(g\)](#).
- l) Pricing for additional services category, including those involving third-party/marketplace components, shall be determined by NICSI through one or more of the following methods, as deemed appropriate:
 - i. Market Survey
 - ii. Limited Tendering
 - iii. Reference Rates from Other Government Departments/Agencies

The proposed rates, arrived at through any of the above methods, shall be subject to review and approved by competent authority to ensure fairness, transparency, and alignment with prevailing market conditions.
- m) During the validity of the empanelment including the extended period, if any, if the Service Provider quotes, sells or exhibits written intention to sell any empanelled item of the same or equivalent configuration/specification to any other Department/Organization at a price lower than the price empanelled for NICSI under same terms and conditions as defined in this RFE, the Service Provider shall voluntarily pass on the price difference to NICSI. The effective date will be date of selling / intent to sell at a lower rate.

9.3. Security Deposit for Empanelment

- a. The selected bidder(s) will submit the security deposit in the form of an Account Payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, Bank Guarantee, Bankers

Cheque from a Commercial bank or online payment in an acceptable form for the duration of the empanelment plus 3 months or extended period if any (with 3 months add on period), in favour of NICSI, New Delhi.

- b. The bidder shall furnish a Security Deposit of -

Tier 1	Rs. 5 Crore
Tier 2	Rs. 15 Crore
Tier 3	Rs. 30 Crore

- c. NICSI will have the right to forfeit the security deposit if the empanelled agency fails to meet the terms and conditions of the REF document or perform any other obligation under the contract, fails to execute the work orders issued by NICSI.
- d. Apart from this NICSI also reserves the right to cancel the empanelment of the selected agency in case of repeated default.
- e. Empanelled agencies shall be required to submit Security Deposit within 14 days of issuance of Empanelment letters by NICSI.
- f. The Security Deposit should remain valid for a period of 15 months beyond the date of completion of all contractual obligations of the agency i.e. Empanelment/Extension duration.
- g. In the event wherein the Empanelment is extended by NICSI beyond 2 years, the selected agency shall ensure submission of a fresh Security Deposit within 14 days of issuance of letter for extension of Empanelment by NICSI.
- h. The Validity of this Security Deposit shall also be for an additional period of 15 months beyond the period of extension of Empanelment.
- i. The BG will be released without any accrued interest after the empanelment or execution of all pending POs whichever is later.

9.4. Performance Bank Guarantee (PBG)

- a. The selected Service Provider shall be required to furnish a **Performance Bank Guarantee equivalent to 5% (Five Percent) of the Work Order/Purchase Order value for each WO/PO issued** during the empanelment period.
- b. Empanelled agencies shall submit the PBG within 30 days of issuance of PO by NICSI.
- c. PBG will be in the form of an Account Payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, an unconditional and irrevocable Bank Guarantee, Bankers Cheque from a Commercial bank or online payment in an acceptable form drawn in the name of National Informatics Centre Services Inc. (NICSI), New Delhi.
- d. The PBG should remain a period of **180 (One Eighty days)** beyond the date of completion of all contractual obligations of the supplier.
- e. The Performance Bank Guarantee must be submitted after award of contract but before signing of contract.

- f. The successful service provider must renew the Performance Bank Guarantee on same terms and conditions for the period up to contract including extension period, if any.
- g. Performance Bank Guarantee would be returned (without any accrued interest) only after successful completion of tasks assigned in the PO and only after adjusting/ recovering any dues recoverable/ payable from/ by the Service Provider on any account under the contract.
- h. NICS I will have the right to forfeit the PBG along with the Security Deposit without assigning any reasons if the selected agency defaults or deemed to have defaulted or in the case of non-acceptance of the purchase orders and thereafter the empanelment will be cancelled.
- i. In the event wherein a PO is released by NICS I for project renewal, or a fresh PO is released, the bidder shall ensure extension / submission of PBG with 15 days of issuance of the PO.
- j. In the event of default in submission of PBG within the stipulated time, the agency shall be liable for a penalty amounting to **0.1% (Zero Point One Percent)** of the PO value per day delay with a Maximum penalty capping of PBG Value.

10. PLACEMENTS OF WORKORDERS

NICS I may place the work orders with the empanelled agencies for its own requirement or for its projects on behalf of its clients.

- a. This REF is for empanelment of multiple agencies in three different categories – Tier 1, Tier 2 and Tier 3, based on complexity, and specialization of services provided by the agencies. For empanelled bidders within a category, pricing will be auto-calculated using the NICS I list price platform. Accordingly, the allocation of projects (purchase orders) within each category will be as per NICS I/User department. However, NICS I reserves the right to allocate projects (purchase orders) to any other eligible bidder, considering factors such as performance, location, project diversity, or any other relevant parameters as deemed necessary.
- b. The Work Order may encompass the complete scope of work or may require few services. Depending on the requirement, the work orders may be placed to the empanelled agency for the specific scope of work. In the document, the work order can be read as work order/Purchase order.
- c. On receipt of request from a User department, NICS I would inform the User Department about the Empanelled agencies and the GFR compliant procedure followed in the empanelment.
- d. The Terms of Reference/ Scope of Work will be shared among all Empanelled agencies in a specific category, and they would be invited by the Committee to make presentations and submission of technical proposal and financial effort estimate in a separate sealed envelope regarding the project under consideration. The presentations may be evaluated objectively, based on which the most suitable agency may be assigned the work by NICS I, on the recommendation of the above Committee. There should be full participation and involvement of the User Department in the process of selection of agency. For assignment of work to Empanelled agencies, the

above mentioned Standard Operating Procedure (SOP) is followed or implementation of new guidelines from time to time.

- e. The proposal of the selected agency along with necessary supporting document/ minutes of meeting are then forwarded to NICSI by the user department for issuance of Proforma Invoice (PI).
- f. Once the requisite funds are transferred to NICSI against issued PI, the Work Order will be placed on the selected agency as per the terms and conditions of the empanelment and scope of work.
- g. NICSI may place work orders till the last date of empanelment or extension period, for a period up to beyond one year from the last date of empanelment or extension period.
- h. Empanelled agencies deploying hardware and software for the delivery of cloud services shall ensure that all components of their solution are free from any malicious code, hidden threats, or vulnerabilities that could compromise the integrity, confidentiality, or availability of government data and systems. Non-compliance or detection of any malicious component at any stage may lead to disqualification, blacklisting, and/or legal action as deemed appropriate by NICSI/User department.
- i. Customization of SLAs: The User Department shall have the right to define, add, or modify specific Service Level Agreements (SLAs) at the time of placement of the Work Order, based on the nature, criticality, and performance expectations of the project. Such modifications shall remain consistent with the overall framework and minimum service levels defined in this RFE and shall be mutually agreed upon by the selected agency and the User Department.
- j. Initial Project Allocation by Tier: To ensure fair opportunity and optimal utilization of empanelled Cloud Service Providers (CSPs), the first project allocation under this engagement shall be made as per the following tier-wise value thresholds:
 - i. Category Tier 1: Eligible for initial project allocation up to INR 10 Crore
 - ii. Category Tier 2: Eligible for initial project allocation up to INR 20 Crore
 - iii. Category Tier 3: Eligible for initial project allocation up to INR 40 Crore

The above thresholds are applicable for awarding the first project in each tier category post-empanelment. Subsequent allocations shall be based on performance, capacity, compliance, and NICSI's discretion.

11. ADDITION OF NEW SERVICES

- a. In case an empanelled agency proposes to add new services or products under an existing service category during the empanelment period, the overall discount percentage finalized for that service category shall be applicable to the newly added service/product. For example, as cited in the table below, for any new service or product added under the 'Compute as a Managed Service (Tier-1)' category, a discount of **39%** shall be applied to the listed/base price of such new service/product.

S. No.	Service Name / Type of Service	Configuration /Description of Service	Specifications of required Service	Unit of Measure ment	List Price (Rs.)	Offered Price (Rs.)	Calculated Discount (%)*
A. Compute as Managed Service (Tier-1)							

1	Production Grade Virtual Machine	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Monthly / 730	100	80	20%
2			VM - 2 vCPU, 8GB RAM	Monthly / 730	200	120	40%
3			VM - 2 vCPU, 16GB RAM	Monthly / 730	400	220	45%
4			VM - 4 vCPU, 8GB RAM	Monthly / 730	800	400	50%
Discount in Service Category							39%

- a. In case of addition of a new services category in a specific 'Tier category', the overall weighted average of all the service categories of that respective Tier will be applicable to the new service category and their services/products.
- b. All such additions shall be subject to approval by NICSI and must comply with the technical and security standards outlined in the RFE.

12. PAYMENT TERMS & SCHEDULE

- a. Payment will be made in Indian Rupees only.
- b. NICSI shall make payment to either the Managed Service Provider (MSP) or the Cloud Service Provider (CSP), as per the preference of the bidder.
- c. The billing for cloud services will be based on actual utilization of infrastructure.
- d. The payment to the service provider will be made on monthly/quarterly basis depending upon the actual duration of services rendered at NICSI/User department after availing service.
- e. If the service provider is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the service provider.
- f. The service provider will submit Pre-receipted bills in triplicate (having details of concerned work-order number, Date and Project-Number of NICSI) on monthly/quarterly basis in the name of NICSI-New Delhi by the 10th day of the succeeding month along with the individual's Monthly Satisfactory Performance Report(s) duly signed by NICSI/User department Project coordinator. Payment will be made within 30-45 days of submission of the Bill along with all the completed documents and after deducting the applicable penalty if any.
- g. Payments shall be made subject to deductions of any amount for which the service provider is liable under the RFE conditions. Further all payments to service provider will be made subject to deduction of TDS (Tax deduction at Source) applicable to deployment of professionals as per the income Tax Act, 1961, and also applicable penalty & other taxes, if any, as per Government of India rules.
- h. It is the bounden duty of the empanelled service provider to regularly pay the deployed manpower their entitlements like monthly salaries/ wages/ annual increment/ EPF/ ESI/

Bonus/ Medical Insurance/ Accidental Insurance etc. as may be applicable and submit the proof thereof to NICSI along with Service Provider Invoices for the processing of the bills.

- i. In case the submission of monthly bills to NICSI is delayed by the service provider beyond 15 days from the last day of the month in which the services has been provided, the entire liability towards payment of interest/penalty to the tax authorities would be borne by the respective service provider; so that NICSI is not burdened unnecessarily with this amount/penalty etc. The entire amount will be deducted from the payment due to respective service provider.
- j. Pre-receipted bills shall be submitted in triplicate in the name of:

National Informatics Centre Services Inc.,
Hall No. 2&3, 6th Floor, NBCC Tower,
15 Bhikaji Cama Place,
New Delhi –110066.

13. SERVICE LEVEL REQUIREMENTS (SLAs)

The purpose of Pre-defined Service Level Agreement (SLA's) is to ensure quality and standards of operation and specify performance criteria that shall be adhered to by the selected bidder during the Operation & Maintenance period of the project (and extended period of project as applicable). Definitions applicable for SLA and Penalty:

- a) Actual Uptime means, the aggregate number of hours in the month during which the individual service is available for use by Purchaser.
- b) Downtime means, the aggregate number of hours in the month during which the individual service is unavailable for use by Purchaser.
- c) Scheduled Maintenance Time means the aggregate number of hours in the month during which the individual service, is unavailable for use by Purchaser, due to Preventive & Scheduled Maintenances for cloud infrastructure, OS patching and up-gradation subjected to prior approval of the purchaser.
- d) Monthly Payment means the amount payable in the particular month (excluding GST), for services rendered by the Service Provider under this contract, before application of any deductions.

13.1 SLAs (Service Legal Agreement)

The general Service Level Agreements (SLAs) applicable during the empanelment period are outlined in this section. However, NICSI or the User Department may define **project-specific SLAs** at the time of issuing the RFQ, if deemed necessary. In the absence of project-specific SLAs, the general SLAs specified herein shall remain applicable by default. The key service level objectives pertaining to the cloud services, as well as the interfaces between NICSI/User Department and the MSP, are detailed below:

- a) **Self-service provisioning:** The MSP/CSP shall offer self-service provisioning capabilities for virtual machines, storage, and other cloud services through an intuitive programmatic interface (API/CLI) or management console. The solution must enable departments to efficiently provision, scale, and manage infrastructure resources based on specific project requirements. Bidders shall be responsible for the design and provisioning of the necessary cloud infrastructure in the form of IaaS, PaaS, or SaaS, as required for each project.

- b) **Availability:** Availability refers to the extent to which the cloud service is accessible and usable on demand by authorized users. It is a critical service level objective, indicating whether the service is operational and functioning as intended. The minimum availability requirement for the cloud service is 99.5% uptime per month, excluding periods of scheduled maintenance. Scheduled maintenance activities must be communicated to NICS/ User Department at least **15 days in advance**, and such maintenance-related downtime shall **not exceed two (2) days** per month. In the event that actual availability falls below the stipulated threshold, the MSP/CSP shall be subject to penalties as specified in [Section 14](#) of this document.
- c) **Performance:** This section outlines the common Service Level Objectives (SLOs) associated with the performance of cloud services and the interaction between the cloud service provider and the customer. These objectives are critical for monitoring and evaluating service quality throughout the engagement. Key indicative performance parameters under the SLA shall include responsiveness in provisioning new virtual machines (VMs), response time for processing transactions, and the performance of storage services such as the spinning of object and block storage. These parameters will serve as benchmarks to assess the service provider's compliance and operational efficiency.
- d) **Security:** Security incidents may include, but are not limited to, malware attacks, denial-of-service (DoS) attacks, intrusions, and any form of security breach such as data theft, loss, or corruption. Given the critical importance of security in cloud service delivery, stringent standards shall be enforced to govern all aspects of security management. Any security incident that results in a disruption of the availability or integrity of the cloud service shall be subject to penalties, as per the applicable terms and conditions. The MSP/CSP shall maintain robust security measures to protect the cloud infrastructure from security incidents, including malware attacks, denial of service (DoS) attacks, intrusions, and data theft, loss, or corruption. The MSP/CSP shall:
- i. Notify NICS/ User departments within 1 hour in case of any security breach.
 - ii. Ensure that all data is encrypted at rest and in transit, with strict access controls.
 - iii. Provide regular security audits and reports to NICS/ User departments.
 - iv. Failure to adhere to these standards will result in penalties as outlined in [Section 14](#).
- e) **Disaster Recovery and Data Backup Management:** This category pertains to Business Continuity Management (BCM) and Disaster Recovery (DR), which are essential for ensuring the resilience and reliability of cloud services. Disaster recovery refers to the cloud service provider's ability to maintain service availability and data accessibility in an acceptable form over a defined period following a disruptive event or disaster. Scheduled maintenance and planned downtime are typically accounted for during the design of the Service Level Agreements (SLAs). This category also encompasses the service provider's capability to prevent data loss and ensure swift recovery in the event of system failures or unforeseen disruptions. The MSP/CSP shall ensure disaster recovery (DR) capabilities to maintain service continuity and data availability in case of failure. The MSP/CSP must implement regular backup processes to ensure that data is backed up and recoverable. In the event of a disaster, the MSP/CSP must restore services and data within the specified RTO and RPO. Failure to meet these objectives will result in penalties as per [Section 14](#). The two primary service level agreements (Please refer [Table 13.5 \(a\)](#): SLA for specific SLAs) which needs to be addressed here are –
- i. RPO – recovery point is the maximum allowable time between recovery points and
 - ii. RTO – recovery time is the maximum amount of time a business process may be disrupted after the disaster.
- f) **Audit & Monitoring:** Audit and Monitoring refers to the structured and procedural approach aimed at assessing and enhancing the effectiveness of processes and control mechanisms. As

part of the empanelment requirements, MeitY mandates that Cloud Service Providers (CSPs) possess and maintain key certifications, including ISO 27001:2013, ISO 20000:1, ISO 27017, ISO 27018, and TIA-942-B / UPTIME (Tier-3 or higher). Service Level Agreements (SLAs) under this category shall be used to monitor the continued validity and compliance with these certifications. Furthermore, the SLA shall include provisions for timely notifications to NICSI/User Department in the event of disruptions related to patch updates, budgetary issues, or non-resolution of audit observations.

- g) **Measurement and Monitoring:** The MSP/CSP shall provide monthly service level reports, including detailed performance metrics, availability, and incident reports. Failure to submit timely or accurate reports may lead to penalties as specified in [Section 14](#). The reports should:
- i. Be delivered to NICSI/User department within [insert time frame, e.g., 10 business days] after the end of the month.
 - ii. Include data on downtime, performance metrics, security incidents, and compliance with SLAs.
 - iii. Include an analysis of any SLA breaches along with the root cause and corrective actions taken.

The following clauses pertain to measurement and monitoring:

- i. **SLA Monitoring Frequency:** Service Level Agreement (SLA) parameters shall be monitored on a **quarterly basis** in alignment with the specific requirements of each SLA parameter. However, in the event of significant degradation in system/service performance at any time during the contract period, and where immediate corrective measures are not implemented to the complete satisfaction of NICSI/User Department, the Department reserves the right to take appropriate disciplinary action, including termination of the contract.
 - ii. **Service Level Reporting:** A comprehensive set of service level performance reports shall be made available to NICSI/User Department on a **monthly basis**, or at other intervals as specified by project requirements.
 - iii. **Monitoring Tools and Access:** SLA compliance shall be tracked using automated monitoring tools, which must be tailored to meet the SLA measurement requirements. The Service Provider shall provide access to these tools and may deploy additional utilities to ensure accurate and automated SLA report generation. The tools must generate detailed SLA Monitoring Reports at the **end of each month**, which shall be shared with NICSI/User Department. Full access to the monitoring tools/portals (including all related scripts, data, and reports) shall be granted to NICSI/User Department, which also retains the right to audit the tools and scripts regularly.
 - iv. **Measurement Review:** The measurement methodology, criteria, and logic for SLA evaluation shall be subject to periodic review and approval by NICSI/User Department.
 - v. **Non-Compliance Handling:** In the event of any SLA breach, the Service Provider shall submit a Performance Improvement Plan (PIP) along with a detailed Root Cause Analysis (RCA) for review and approval by NICSI/User Department.
- h) **Reviews:** The Service Level Agreements (SLAs) may need to be tailored or modified based on specific project requirements. Accordingly, NICSI/User Department shall ensure that the contractual agreement includes appropriate provisions that allow for the revision or customization of SLAs as needed to align with project objectives and operational needs.

- i. During the contract period, changes to the SLA—including adjustments to the measurement methodology, logic, criteria, or the addition, modification, or removal of specific parameters—may be made subject to the mutual consent of both parties, namely the User Department and the Service Provider.
- ii. The User Department and Service Provider shall ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of the User Department and Service Provider in accordance with the Change Control Schedule.
- iii. The SLAs may be reviewed on an annual basis by the User Department in consultation with the Service Provider and other agencies.
- iv. All the SLA penalty calculations should be done for the mentioned calendar month.

During the contract period, the SLAs may be subject to review and modification based on evolving project needs. Any changes to the SLA, including alterations to measurement methodology, criteria, or the addition/deletion of parameters, will:

- i. Be agreed upon by both NICS/ User department and the MSP/CSP in writing.
- ii. Be based on mutual consent and documented in a formal amendment to the agreement.
- iii. Be aligned with the project's goals and objectives.

13.2 Support/Helpdesk Tool and SLA Management Tool

- a) Cloud IT infrastructure SLA monitoring shall be integrated through an automated, centralized Helpdesk and SLA Monitoring Tool provided by the bidder. The bidder shall utilize this tool to manage tickets and monitor SLAs related to the cloud services. The bidder will be responsible for timely resolution of tickets and ensuring compliance with the agreed SLAs, which fall within their scope of work. The SLA monitoring tool is expected to include the following key features:
 - i. Track and resolve tickets within the agreed SLA timelines.
 - ii. Provide automated reports on SLA compliance, including response and resolution times on a Weekly, Monthly, Quarterly basis.
 - iii. SLA reporting should be based on automated logs with minimal manual interventions. Be capable of generating SLA compliance reports for NICS/ User department periodically.
 - iv. Well-defined processes should be implemented for those SLAs that require manual intervention for measurement and reporting. In such cases, the SLA measurement methodology should be discussed and agreed upon with the purchaser.
 - v. The Bidder shall implement the SLA Monitoring System to measure performance against each of the indicators listed under SLAs specified in the REF. The SLA Monitoring System shall be reviewed by the purchaser before usage.
 - vi. Should automatically document problems and interruptions of services and provide the consolidated violations as per the SLA
 - vii. Should allow NICS/ User department to audit the tool and access raw data as necessary.
- b) However, It will be final decision of NICS/ User department to continue, with the existing tool or NICS/ User department may ask bidder to integrate/onboard to a single monitoring platform as per the requirement.

13.3 Incident Severity Levels & Critical Services

- a) **Severity Level 1:** Environment is down, or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of

end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available.

- b) **Severity Level 2:** Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.
- c) **Severity Level 3:** Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.
- d) **Critical Services:** Critical service may be defined as Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Security Components, etc.

13.4 Contract Compliance and Resolution Mechanism

- i. In case of delays due to reasons beyond the control of the MSPs/CSPs, the User department may consider the delay and extend the timeline at its sole discretion.
- ii. If the SLA dependency for resolving the ticket is on a third party, then the overall time to resolve will factor this delay. However, the CSP/MSP must make all reasonable efforts to minimize such delays and ensure timely resolution in accordance with the agreed SLAs.
- iii. Response Time: Average Time taken to acknowledge and respond, once a ticket / incident is logged. This will be calculated for all tickets/ incidents reported within the reporting month, against that category.
- iv. Resolution Time: Average Time taken to resolve the reported ticket / incident from the time of logging. This will be calculated for all tickets/ incidents reported within the reporting month, against that category.
- v. Resolution Mechanism: In case the service provider has any complaint(s) on the categorization of the registered ticket(s), the same may be put up by the service provider to the purchaser for resolution, within 7 days of the month end, with necessary supporting justification(s). The final decision regarding categorization of the registered Support/Helpdesk ticket(s) shall rest with the purchaser.

13.5 Monthly Service Level Availability

The Service Level Availability (SLA) requirement which needs to comply to by the service provider is given in the below table. The table shows the Service Level Objectives and corresponding Definition, Target and applicable Penalties for breach of SLAs. The SLAs will be calculated on Monthly basis for the project in the subsequent RFQs.

The formula to calculate the **percentage of service availability**, factoring in both **actual uptime** and **scheduled maintenance**, relative to the total hours in a given month is as follows:

$$\text{Availability} = [(\text{Actual Uptime} + \text{Scheduled Maintenance Time}) / \text{Total No. of Hours in the Month}] \times 100$$

Table 13.5 (a): Service Level Availability (SLA)

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
Availability					

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
1	Availability of each cloud service (Applicable for all Cloud Service as defined in BoQ)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use	$\{[(\text{Uptime Hours in the calendar month} / (\text{Total No. of Hours in the calendar month} - \text{Scheduled Downtime in the calendar month}))] \times 100\}$	Availability for each of the cloud service $\geq 99.5\%$ excluding archival storage	Default on any one or more of the provisioned services resulting in impact to overall availability and uptime will attract penalty as indicated below: A). $< 99.5\%$ to $\geq 99.00\%$ - 10% of Quarterly Payment of the work order value B) $< 99.00\%$ to $\geq 98.50\%$ - 15% of Quarterly Payment of the work order value C) $< 98.50\%$ to $\geq 98.00\%$ - 20% of Quarterly Payment of the work order value D) $< 98\%$ - 30% of the Quarterly Payment of the work order value. In case the services are not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					Quarterly Payment of the work order value.
2	Availability of regular reports (SLA, Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted to the Purchaser within 5 working days from the end of the month.	Submission of reports	Regular reports should be submitted to the Purchaser within 5 working days from the end of the month.	Penalty as indicated below (per occurrence): A) <11 working days to >= 6 working days - 2% of Quarterly Payment for the work order value B) <16 working days to >= 11 working days - 4% of Quarterly Payment for the work order value C) For the delay beyond 15 days, penalty of 5% of the Quarterly Payment for the work order value.
3	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually, available for use	Uptime Calculation for the calendar month: $\{[(\text{Uptime Hours in the calendar month} / (\text{Total No. of Hours in the calendar month} - \text{Scheduled Downtime in the calendar month}))] \times 100\}$	Availability of the Cloud Management Portal of CSP >=99.5%	Default on availability of cloud management portal on every occurrence will attract penalty as indicated below:) A) <99.5% to >= 99.00% - 10% of Quarterly Payment of

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					<p>the work order value</p> <p>B) <99.00% to >= 98.50% - 15% of Quarterly Payment of the work order value</p> <p>C) <98.50% to >= 98.00% - 20% of Quarterly Payment of the work order value</p> <p>D) <98% - 30% of the Quarterly Payment of the work order value.</p> <p>In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the Quarterly Payment of the work order value.</p>
Performance					
4	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core).	Measurement shall be done by analyzing the log files.	95% within 5 minutes	<p>Penalty as indicated below (per occurrence):</p> <p>A) <95% to >= 90.00% - 5% of Quarterly Payment of the work order value.</p>

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					B) <90% to >= 85.0% - 10% of Quarterly Payment of the work order value. C) <85% to >= 80.0% - 15% of Quarterly Payment of the work order value. D) <80% - 20% of the Quarterly Payment of the work order value
5	Spinning up the Object Storage	Time to spin up Object Storage.	Measurement shall be done by analysing the log files.	98% within 15 minutes	A) <98% to >= 95.00% - 5% of Quarterly Payment of the work order value B) <95% to >= 90.0% - 10% of Quarterly Payment of the work order value. C) <90% to >= 85.0% - 15% of Quarterly Payment of the work order value. D) <85% - 20% of the Quarterly Payment of the work order value
6	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM.	Measurement shall be done by analyzing the log files.	98% within 15 minutes	Penalty as indicated below (per occurrence):

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					A)<98% to >= 95.00% - 5% of Quarterly Payment of the work order value B)<95% to >= 90.0% - 10% of Quarterly Payment of the work order value C)<90% to >= 85.0% - 15% of Quarterly Payment of the work order value D)<85% - 20% of the Quarterly Payment of the work order value.
7	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage.	Measurement shall be done by analyzing the log files and Cloud Service (API) reports	No more than 15 minutes lag between usage and Cloud Service (API) reporting, for 99% of Cloud Services consumed by the client.	Penalty as indicated below (per occurrence): A) <99% to >= 95.00% - 1% of Quarterly Payment of the work order value B) <95% to >= 90.0% - 2% of Quarterly Payment of the work order value. C) <90% to >= 85.0% - 3% of Quarterly Payment of the work order value.

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					D) <85% - 5% of the Quarterly Payment of the work order value.
8	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24 Hrs of actual usage.	Measurement shall be done by analyzing the log files and Cloud Service (API) reports and Invoices.	No more than 24 Hrs of lag between availability of cost details and actual usage, for 99% of Cloud Services consumed by the Purchaser	Penalty as indicated below (per occurrence): A) <99% to >= 95.00% - 1% of Quarterly Payment of the work order value. B) <95% to >= 90.0% - 2% of Quarterly Payment of the work order value C) <90% to >= 85.0% - 3% of Quarterly Payment of the work order value. D) <85% - 5% of the Quarterly Payment of the work order value.
Security and Integrity					
9	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with Purchaser within 5 working days of vulnerability identification.	Measurement period is calendar month.	Percentage of timely vulnerability reports shared with Purchaser within 5 working days of vulnerability identification >= 99.95%	Penalty as indicated below (per occurrence): A) <99.95% to >= 99.00% - 10% of Quarterly Payment for the work order value. B) <99.00% to >= 98.00% -

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					20% of Quarterly Payment for the work order value. C) <98% - 30% of Quarterly Payment for the work order value.
10	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. High Severity – Perform vulnerability correction within 30 days of vulnerability identification. Medium Severity - Perform vulnerability correction within 60 days of vulnerability identification. Low Severity - Perform vulnerability correction within 90 days of vulnerability identification.	Measurement period is calendar month.	Maintain 99.95% service level	Penalty as indicated below (per occurrence): A)<99.95% to >= 99.00% - 10% of Quarterly Payment for the work order value. B)<99.00% to >= 98.00% - 20% of Quarterly Payment for the work order value. C) <98% - 30% of Quarterly Payment for the work order value.
11	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)		No Breach	For each breach/data theft, penalty will be levied as per following criteria. Severity 1 - Penalty of Rs 15 Lakh per incident. Severity 2 - Penalty of Rs 10 Lakh per incident. Severity 3 - Penalty of Rs

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					5 Lakh 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, NICS/ User Department reserves the right to terminate the contract.
12	Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		Post incident has occurred and has been resolved	Average within 10 Working days	2% of periodic payment for each RCA delay beyond mentioned target.
Helpdesk Support and Incident Management					
13	Incident Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels (Online tool provided by MSP).	This is calculated for all tickets/ incidents reported within the reporting month.	95% within 30 minutes	a) < 95% & >= 90% (3% of the periodic payment) b) < 90% (5% of the periodic payment)
14	Time to Resolve - Severity 1 (for definition refer to table below)	Time taken to resolve the reported ticket/incident from the time of logging		For Severity 1, 98% of the incidents shall be resolved within 4 Hours of the reporting	a) < 98% & >= 90% (3% of the periodic payment) b) < 90% (5% of the periodic payment)
15	Time to Resolve - Severity 2 (for definition refer to table below)	Time taken to resolve the reported ticket/incident from the time of logging		95% of Severity 2 within 8 hours of Incident reporting	a) < 95% & >= 90% (3% of the periodic payment) b) < 90% & (5% of the

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					periodic payment)
16	<p>Helpdesk Ticket response time</p> <p>Response Time = Average time taken to create a fault / request ticket from the time of notification about the fault/request.</p>	Monitoring report generated by the EMS/ Call logs	<p>Performance Rate (%) = $[1 - (\text{Total Number of Requests with Response Time Exceeding Threshold} / \text{Total Number of Requests})] \times 100$</p> <p>Frequency: Monthly</p>	>=95% within 30 minutes	<p>For availability 95% or higher -</p> <p>a. < 95% & >= 93%: Penalty of ₹50,000/-</p> <p>b. < 93% & >= 91%: Penalty of ₹75,000/-</p> <p>For availability below 91% - Penalty @ ₹1,00,000/- for every 2% (or part thereof) reduction of availability below 95%.</p>
17	<p>Helpdesk Ticket closure time</p> <p>Ticket Closure Time = Average time taken to Close the trouble/request ticket</p>	Monitoring report generated by the EMS	<p>Performance Rate (%) = $[1 - (\text{Total Number of Requests with Response Time Exceeding Threshold} / \text{Total Number of Requests})] \times 100$</p>	>=95% within 4 hours	<p>No penalty for closure greater than 95% of the tickets.</p> <p>a. < 95% & >= 93%: Penalty of ₹50,000/-</p> <p>b. < 93% & >= 91%: Penalty of ₹75,000/-</p> <p>For closure of tickets below 91% -</p> <p>a. Penalty @ ₹1,00,000/- for every 2% (or part thereof) reduction in closure of tickets below 95%.</p>
18	Incorrect Closure of the Helpdesk tickets	ITSM Tool Report provided by the EMS	Analysis of the tickets from	For each incident of	A penalty of INR 10,000/-

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
			each category of the tickets	incorrect trouble ticket closure.	for each incorrect trouble ticket closure detected.
Disaster Recovery (Applicable on DR services)					
19	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Recovery time is the maximum amount of time a business process may be disrupted after the disaster.	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <= 4 hours Government Department may specify more stringent RTO based on its application requirements	10% of Quarterly Payment of the work order value per every additional 2 (two) hours of downtime.
20	RPO (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Recovery point is the maximum allowable time between recovery points.	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours Government Department may specify more stringent RPO based on its application requirements.	10% of Quarterly Payment of the work order value per every additional 2 (two) hours of data loss.
21	DR Drills		At least two DR drills in a year (once every six months) or as per the agreement	At least two DR drills in a year (once every six months) or as per the agreement	A) No of DR Drills = 1 - 1% of the Yearly Payment of the work order value. B) No of DR Drills = 0 - 2% of the Yearly Payment of the work order value. These will be measured every six months and the liquidated damage will be levied at the end of year.

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
22	Data Migration		Migration of data from the source to destination system	Error rate < .25%	<p>A) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the work order value.</p> <p>B) Error Rate > 0.30% & <=0.35% - 2% of the Quarterly Payment of the work order value.</p> <p>C) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the work order value.</p> <p>For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the work order value will be levied as additional liquidity damage.</p>
Backup & Restore					
23	Configuration Backup (as specified in Section Backup Solution) of each of the Systems & Subsystems	Source: Daily Report from the backup automation system which is configured to execute the backups.	Methodology: Success Rate (%) = (Total Number of Successful back ups / Total Number of	The success rate shall be better than 99% for all the systems & and subsystems	Per day INR 10,000 of non-availability of daily backup

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
			backup events) x 100	of the solution both virtual and physical.	
24	Accuracy of the backup process, ensuring 100% contents of the target source are copied to the backup storage	Source: Daily Report from the backup automation system which is configured to execute the backups.	Accuracy Rate (%) = (Total Number of files that have been backed up from the source folder/ Total Number of files that have to be backed up from the source folder) x 100	The success rate shall be 100% for all the backups	Penalty of INR 10,000 for each missing file in the daily backup
25	Restoration of configuration (as specified in Section Backup Solution) of each of the Systems & Subsystems	Source: Select 10 instances across different categories of equipment that shall be randomly selected for restoration	Success Rate (%) = (Total Number of Successful Restoration / Total Number of Restoration attempts) x 100 Frequency: Restoration tests to be conducted once in a quarter	The success rate shall be better than 99% for all the categories of systems & subsystems	INR 50,000 per instances of failure
Audit & Monitoring					
26	Patch Application	Patch Application and updates to underlying infrastructure and cloud service. Measurement shall be done by analysing security audit reports		95% within 8 Hrs of the notification	Penalty as indicated below (per occurrence): A) <95% to >= 90.00% - 5% of Quarterly Payment of the work order value. B) <90% to >= 85.0% - 10% of Quarterly Payment of the work order value. C) <85% to >= 80.0% - 15% of Quarterly Payment of

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					the work order value. D) <80% - 20% of the Quarterly Payment of the work order value.
27	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage-based threshold.	Measurement shall be done by analysing the log files.	99% within 10 mins of crossing the threshold	Penalty as indicated below (per occurrence): A) <99% to >= 95.00% - 0.25% of Quarterly Payment of the work order value. B) <95% to >= 90.0% - 0.5% of Quarterly Payment of the work order value. C) <90% to >= 85.0% - 0.75% of Quarterly Payment of the work order value. D) <85% - 1% of the Quarterly Payment of the work order value.
28	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project duration. Service Provider should ensure the		All certificates should be valid during the Project duration	Delay in sustenance of certifications A) > 1 day & <= 5 days - 1% of the Quarterly Payment of the work order value

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
		sustenance / renewal of the certificates			B) > 5 day & <= 15 days - 2% of the Quarterly Payment of the work order value C) > 15 day & <= 30 days - 5% of the Quarterly Payment of the work order value D) > 30 days, 10% of the Quarterly Payment of the work order value
29	Non-closure of audit observations	No observation to be repeated in the next audit		All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit A) > 0 % & <= 10% - 5% of the Quarterly Payment of the work order value. B) > 10 % & <= 20% - 10% of the Quarterly Payment of the work order value. C) > 20 % & <= 30% - 20% of the Quarterly Payment of the work order value. D) >30% - 30% of the Quarterly Payment of

S. No	Service Level Objective	Definition	Measurement Methodology	Target	Penalty
					the work order value.

14 PENALTY

- a. For the NICS/ User Departments to ensure that the Cloud Service Providers or Managed Service Provider adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on CSP. In case these service levels cannot be achieved at service levels defined in the agreement, the departments will invoke the performance related penalties.
- b. Payments to the Service Provider to be linked to the compliance with the SLA metrics laid down in the agreement. The penalty in the percentage of the monthly payment has been as indicated against each SLA parameter in the [Table 13.5 \(a\)](#).
- c. If outage is due to CSP except application related malfunction, then 10% penalty of month bill will be imposed.
- d. Payments to be linked to the compliance with the SLA metrics laid down in the agreement. NICS/ may constitute a committee to analyze and review the SLA as needed. To illustrate calculation of penalties, an indicative example is provided below.
For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Monthly/Quarterly Payment is deducted from the total of the Monthly/Quarterly bill and the balance paid to the CSP.
- e. If the penalties are to be levied in more than one SLA, then the total applicable penalties are calculated and deducted from the total of the Monthly/Quarterly bill and the balance paid to the MSP.
- f. For ex: SLA1 =7% of the Monthly/Quarterly Payment, SLA12=10% of the Monthly/Quarterly Payment, SLA19=2% of the Monthly/Quarterly Payment then, Amount to be paid = Total Monthly/Quarterly bill – {(19% of the Monthly/Quarterly Payment)}.
- g. In case multiple SLA violations occur due to the same root cause or incident, then the SLA that incurs the maximum penalty will be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.
- h. The SLA for availability of Cloud service (defined as availability of all servers, storage and supporting DC infrastructure including network infrastructure and network connectivity) is 99.5% with no unscheduled downtime.
- i. In the event of default in submission of PBG by the Empanelled agency within the stipulated time, the agency shall be liable for a penalty amounting to **0.1% (Zero Point One Percent)** of the PO value per day delay with a Maximum penalty capping of PBG value. No payment against the PO will be made till PBG is submitted.
- j. The Service Provider shall provide skilled manpower as mentioned in the RFQs in position and capable of supporting the deployment and implementation to adhere to the scope of work of the projects. In case, the Service Provider fails to deliver, support or co-operate with the User department, penalty would be levied and deducted from the payment due or from Performance Bank Guarantee.
 - a. If the agency fails to deploy total manpower mentioned in the contract as per the date of joining, up to 15 Days, penalty shall be charged at the rate of **@1 % per day of the total value** and beyond 15 days cancellation of the contract with cancellation charges @ 10% of the order value, in addition to per day penalty.
 - b. If a deployed resource remains absent or takes leave for more than 2 days without informing or taking prior approval, the agency shall substitute within 2 days failing which, **@ 1 % per day of the total value** (excluding service tax etc.) of the absent

resources up to 15 days. Beyond 15 days, cancellation of the contract with cancellation charges @ 10% of the order value, in addition to per day penalty.

- k. The Service provider will be exempted from any delays or slippages on SLA parameters arising out of force majeure event effecting the SLA which is beyond the control of the Service Provider.
- l. In case service provider fails to achieve compliance level of services successively in two quarters or any three quarters in a year, NICS/ User department will reserve the right to re-look at the contract and redefine SLA and penalty clauses to safeguard its interest.
- m. The maximum penalty applicable at any given time, on a cumulative basis within a quarter, shall not exceed 100% of the quarterly payments. Exceeding this limit shall be considered a material breach.
- n. In the event of a material breach, the Cloud Service Provider (CSP) will be granted a cure period of one month, or an extended period as confirmed by the Purchaser, to rectify the breach. Failure to remedy the breach within the stipulated period may result in the issuance of a termination notice and forfeiture of the performance security.
- o. The Service Provider shall only be eligible for payment of approved works done in such a scenario and the decision of NICS/ User department shall be final.
- p. Further, NICS/ User department will be free to cancel the work order and get the work done through an alternate empanelled Service Provider. There shall be no changes in the rates finalized upon award of the project to the alternate Service Provider for the whole period of contract and support.
- q. In the event of a data breach, security breach, or breach of confidentiality, penalty will be imposed. The penalty amount will be determined on a case-by-case basis, considering the nature and impact of the breach.

15 EXIT MANAGEMENT

This clause sets out the provisions, which will apply during the Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

- a. Continuity and performance of the Services at all times including the duration of the agreement and post expiry of the Agreement is a critical requirement of NICS/ User department. It is the prime responsibility of MSP during exit management period and in no way any facility/service shall be affected/degraded. Further, MSP is also responsible for all activities required to train and transfer the knowledge to department (or representative agency of department).
- b. The exit management period starts, in case of expiry of contract, at least 3 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 department or three months after the beginning of the exit management period, whichever is earlier. The cost will be borne by CSP/MSP.
- c. At the end of the contract period or upon termination of contract, MSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of department.

15.1 Exit Management Plan

- a) MSP shall provide department with a recommended “Exit Management SOP” within 90 days of signing of 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.
- b) MSP shall provide support to department for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY under Cloud Services empanelment.
- c) Exit Management Plan will include following but limited to:
 - i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
 - ii. Plans for the communication with such of the CSP, MSP, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project’s operations as a result of undertaking the transfer.
 - iii. Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.
 - iv. Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
 - v. Proposal for necessary setup or institution structure required at department level to effectively maintain the project after contract ending.
 - vi. Training and handholding of department Staff or designated officers for maintenance of project after contract ending.
- d) NICSI/User department will approve this plan after necessary consultation and start preparation for transition.
- e) In the event of any activity triggering the exit clause, a 10% penalty will be imposed, and all ongoing work orders will be terminated.

15.2 Exit Management Services

- a) MSP/CSP shall be responsible for copy all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to department supplied industry standard media.
- b) MSP/CSP shall retain the data / copy of Database for 90 days and MSP/CSP shall ensure that there is no deletion of data for a minimum 90 days beyond the expiry of the contract without any confirmation from department. If data is to be retained beyond 90 days, the cost for retaining the data may be obtained in the commercial quote.
- c) The format of the data transmitted from the MSP/CSP to the department should leverage standard data formats (e.g., OVF, VHD...) whenever possible to ease and enhance portability. MSP/CSP must ensure that the virtual machine format is compatible with other CSP, so that department can migrate from one CSP to other CSP. Department should be able to export the virtual machine from CSP cloud and use that anywhere. CSP shall give provision to import cloud VM template from other CSPs.
- d) CSP shall necessarily support for /establishment of network connectivity to / from other CSPs (within India) if required
- e) CSP shall ensure that all the documentation required by the department for smooth transition (in addition to the documentation provided by the CSP) are kept up to date and all such documentation is handed over to the department during regular intervals as well as during the exit management process. Also ensure that all the documentation required for smooth transition including configuration documents are kept up to date.
- f) Post exits all the data content should be removed to ensure that the data cannot be recovered.

- g) CSP shall address and rectify the problems with respect to migration of the department application and related IT infrastructure during the transition.
- h) CSP shall decommission and withdraw all hardware and software components after the completion of the contract period and formally close the project. This process will be initiated 6 months before the ending of the project contract. If there is a delay in initiating the formalities, the timeline may be extended by a maximum of six months at no additional cost.
- i) At any time during the exit management period, the MSP will be obliged to provide an access of information to department and / or any replacing MSP/CSP 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 material related to implementation of IT Infrastructure Solution for department.
- j) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

16 SPECIAL TERMS & CONDITIONS

16.1. General Conditions

- a. The empanelment under this REF is not assignable by the selected agency. The selected agency shall not assign its contractual authority to any other third party.
- b. As a matter of policy and practice and on the basis of Notification published in Gazette of India dated 14th March, 1998, it is clarified that services and supplies of the agency selected through this REF can be availed by both National Informatics Centre (NIC) and National Informatics Centre Services Incorporated (NICS), as the case may be depending on the project, and the selected agency shall be obliged to render services / supplies to both or any of these organizations as per the indent placed by the respective organization. In other words, the selection procedure adopted in this REF remains applicable for NIC as well, and in the event of rendering services / supplies to NIC, the selected agency shall discharge all its obligations under this REF vis-à-vis NIC.
- c. In case the empanelled agency/bidder is found in-breach of any condition(s) of REF or supply order, at any stage during the course of project deployment period, the legal action as per rules/laws will be taken, as the case may be, including execution of EMD/Bid Securing Declaration, security deposit stipulated in this REF document. The decision of NICS arrived at as above will be final and no representation of any kind will be entertained on the above.
- d. Any attempt by any agency/empanelled bidder to bring pressure of any kind, may disqualify the agency/empanelled bidder for the present REF and the agency/empanelled bidder may also be liable to be debarred from bidding for NICS RFEs/tenders in future for a period of at least three years.
- e. All terms and conditions governing prices and supply given in this REF, as applicable to NICS, will be made equally applicable to NIC.
- f. NICS reserves the right to modify and amend any of the stipulated condition/criterion given in this REF, depending upon project priorities vis-à-vis urgent commitments. NICS also reserves the right to accept/reject a bid, to cancel/abort REF process and/or reject all

bids at any time prior to award of empanelment, without thereby incurring any liability to the affected agencies on the grounds of such action taken by the NICSI.

- g. Any default by the bidders in respect of REF terms & conditions will lead to rejection of the bid with execution of EMD/Bid Securing Declaration and forfeiture of Security Deposit.
- h. The decision of NICSI arrived during the various stages of the evaluation of the bids is final & binding on all bidders. Any representation towards these shall not be entertained by NICSI. Reasons for rejecting a bid will be disclosed only when an enquiry is made by the concerned bidder.
- i. Printed/written conditions mentioned in the REF bids submitted by bidders will not be binding on NICSI.
- j. Upon verification, evaluation/assessment, if in case any information furnished by the bidder is found to be false/incorrect, their total bid/Contract shall be summarily rejected and no correspondence on the same, shall be entertained, and blacklisting the agency for a minimum period of 3 years from participating in NICSI RFEs/tenders.
- k. NICSI will not be responsible for any misinterpretation or wrong assumption by the bidder, while responding to this REF.

16.1. Manpower/Resource Related Conditions

- a. The resources deployed under this REF should be on pay roll of the empanelled MSP/CSP.
- b. The manpower provided by the MSP/CSP shall work as per user departments work schedule.
- c. Neither the MSP/CSP nor its personnel /workmen can be treated as employees of NICSI/User department for any purposes. They are not entitled for any claim, right, preference, etc. over any job/regular employment of NICSI/User department. The agency or its workmen shall not at any point of time have any claim whatsoever against NICSI/User department. The Agency should submit undertaking received from the respective deployed manpower in NICSI / User Department regarding the same.
- d. If NICSI/User Department so recommends, a deployed resource must be replaced by the agency within a period of 10 working days.
- e. It is expressly understood and agreed to between the parties to this agreement that the manpower deployed by the MSP/CSP shall be the employees of the agency for all intents and purposes and in no case there shall be a relationship of employer and employee between the NICSI/User department and the said manpower. The MSP/CSP should submit undertaking received from the respective deployed manpower in NICSI / User Department regarding the same along with appointment letter issued to those manpower/s.
- f. The manpower employed by the MSP/CSP shall have no right, whatsoever, for any appointment in the NICSI/User department in temporarily /ad-hoc /daily wages /regular capacity on the basis of their work in the NICSI/User department.
- g. In case any employee of the MSP/CSP so deployed enters in dispute of any nature whatsoever, it will be sole responsibility of the MSP/CSP to contest the same at appropriate forum(s).

16.2.1. Leave Policy For Deployed Manpower/Resources

- a. The Resources should be stationed in NICSI/User department/Project Location for the entire project period. The Resource has to follow the working hours, working days and Holidays of NICSI/User department.
- b. Resource shall get prior approval of NICSI/User department before leaving NICSI/User department/project location.
- c. Leave entitlement and computation will be effective from date of start of project.
- d. An employee can avail maximum 18 leaves per year on pro-rata basis.
- e. Leave cannot be claimed as an employee's right. Except in case of emergencies, all leave will be granted subject to organization's requirements. A situation will be considered an emergency on a case-by-case basis and will be decided by the Nodal Officer of NICSI/User department/Project.

16.2. Empanelment Exclusivity and Usage Authorization

- a. The empanelment established herein is designated for the exclusive use of National Informatics Centre Services Inc. (NICSI), and its clients. Should any external department or ministry wish to adopt or utilize this empanelment for their own purposes, they must first obtain explicit permission from NICSI. Upon granting such permission, NICSI will levy a usage fee amounting to 5% of the total value of any orders placed under this arrangement. NICSI reserves the right, at its sole discretion, to deny requests for the use of this empanelment or to modify the applicable usage fees. Any empanelled bidder that engages with any User Department using this empanelment without obtaining prior authorization from NICSI, will be subject to **debarment** from empanelment for a period determined by NICSI. Furthermore, such unauthorized engagement will invoke the **exit clause**, leading to immediate termination of the empanelment agreement.
- b. NICSI retains the exclusive authority to empanel additional agencies as deemed necessary, entirely at its discretion, and at any time.

16.3. Cloud Agnostic Services

The Service Provider shall design, develop, manage, and support all services, solutions, and applications, to the extent possible, in a cloud-agnostic manner. This includes ensuring that all architectures, configurations, and codebases are not reliant on the proprietary services or APIs of any single cloud service provider. The Provider shall utilize industry-standard, interoperable technologies and deployment strategies that allow for portability and seamless migration in no time, across multiple cloud environments (e.g., AWS, Azure, Google Cloud Platform, etc.).

Furthermore, the Service Provider shall not implement any technical, contractual, or operational lock-in mechanisms, to the extent possible, that would prevent or significantly hinder the NICSI/User department from migrating to another cloud provider or on-premise infrastructure. Upon request, the Service Provider shall support and assist in such migration within a reasonable period under standard business practices and without undue burden or cost to the Client.

In case of any deviation from the agreed cloud-agnostic approach, the Service Provider shall be obligated to re-engineer and redeploy the affected solution to meet the agreed standards at no additional cost to NICSI/User department. Such remediation shall be completed within a period not exceeding fifteen (15) calendar days from the date of notification.

16.4. Indemnification & Limitation of Liability

The bidder/agency/service provider (the "Indemnifying Party") shall undertake to indemnify NICSI/User department (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively "on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or wilful default in performance or non-performance under this Agreement.

If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by,

- a. Indemnified Party's misuse or modification of the Service.
- b. Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party.
- c. Indemnified Party's use of the Service in combination with any product or information not owned or developed by the Indemnifying Party.

However, if any service, information, direction, specification, or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, the Indemnifying Party shall at its expense and option either:

- a. Procure the right for Indemnified Party to continue using it
- b. Replace it with a non-infringing equivalent
- c. Modify it to make it non-infringing.
- d. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.

The indemnities set out above, shall be subject to the following conditions:

- a. The Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documents or otherwise.
- b. The Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defense of such claim including reasonable access to all relevant information, documentation, and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense.
- c. If the Indemnifying Party does not assume full control over the defense of a claim as provided in this Article, the Indemnifying Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in

such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses.

- d. The Indemnified Party shall not prejudice, pay, or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party.
- e. All settlements of claims subject to indemnification under this Clause will be entered into only with the consent of the Indemnified Party, whose consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement.
- f. The Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages, and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claims or proceedings.
- g. The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss because of such a claim or proceedings.
- h. If the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates; and
- i. If a Party makes a claim under the indemnity set out above in respect of any Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the indemnification obligations set out above.

In no event shall either party be liable for any consequential, incidental, indirect, special, or punitive damage, loss, or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third party claims (other than those set forth in above) even if it has been advised of their possible existence.

The allocations of liability in this Section represent the agreed and bargained for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

16.5. Labour Laws

- a. The agency shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the manpower employed thereof.
- b. Wherever necessary, the agency shall apply for and obtain license as provided under Section 12 of Contract Labour (Regulation and Abolition) Act, 1970, and strictly comply with all the terms and conditions that the licensing authority may impose at the time of grant of license. NICS/User department shall not be held responsible for any breach of the license terms and conditions by the agency.

- c. The agency shall be solely responsible for the payment of wages to the deployed manpower and ensure its timely payment thereof.
- d. The agency shall duly maintain a register giving particulars of the deployed manpower, nature of work, rate of wages, etc.
- e. The agency shall also ensure compliance to all the labour laws, including the following labour legislations:
 - i. Minimum Wages Act *
 - ii. Employees Provident Fund Act *
 - iii. Employees State Insurance Act *
 - iv. Workmen's Compensation Act, if the ESI Act does not apply *
 - v. Maternity Benefit Act *
 - vi. Any other law applicable from time to time.

*Applicable as per respective state
- f. The agency shall be solely responsible to adhere to all the rules and regulations relating to labour practices and service conditions of its workmen and at no time shall it be the responsibility of NICS/ User department.
- g. The empanelled agency is responsible for ensuring that all deployed personnel are adequately insured to cover medical expenses and any contingencies.
- h. In the event of maternity leave, if required by NICS/ User Department, the agency must provide a replacement resource of equivalent calibre to the satisfaction of NICS/ User Department. In line with the Maternity Benefit Act, the user department, as a principal employer, will bear all costs associated with both the replacement and the maternity leave benefits provided to the previously deployed resource.
- i. The agency shall indemnify NICS/ User department against any liability incurred by NICS/ User department on account of any default by the agency or manpower deployed by it.
- j. Neither the agency nor his workmen can be treated as employees of NICS/ User department for any purposes. They are not entitled for any claim, right, preference, etc. over any job/regular employment of NICS/ User department. The agency or its workmen shall not at any point of time have any claim whatsoever against NICS/ User department.
- k. Medical benefits should be provided by the agency to the manpower deployed.

16.6. Termination of Contract

NICS reserves the right to suspend any of the services and/or terminate this agreement in one or more of the following circumstances by giving 30 days" notice in writing:

- a. **Termination For Insolvency, Dissolution etc.:** NICS may at any time terminate the contract by giving written notice to the selected agency without compensation, if the selected agency becomes bankrupt or otherwise insolvent or in case of dissolution of firm or winding up of company, provided that such termination will not prejudice or effect any right of action or remedy which has accrued thereafter to NICS.

- b. **Termination For Default:** NICS I may without prejudice to any other remedy for breach of contract, (including forfeiture of security deposit, Performance Bank Guarantee) by written notice of default sent to the Empanelled agency, terminate the contract in whole or in part after sending a notice to the Empanelled agency in this regard.
 - i. If the Empanelled agency fails to accept the Purchase Order(s);
 - ii. If the Empanelled agency fails to deliver services within the time period specified in the purchase orders or during any extension thereof granted by NICS I;
 - iii. If the Empanelled agency is found to have provided incorrect information to NICS I;
 - iv. If the Empanelment conditions are not met as per the requirements of the application document;
 - v. If the Empanelled agency have made misleading claims about the empanelment status;
 - vi. If the Empanelled agency fails to meet any other terms and conditions under the empanelment contract.
- c. **Termination For Convenience:** NICS I may by written notice, sent to the selected agency, terminate the work order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination will specify that termination is for NICS I's convenience, the extent to which performance of work under the work-order and/or the contract is terminated and the date upon which such termination becomes effective. NICS I reserves the right to cancel the remaining part and pay to the selected agency an agreed amount for partially completed services.
- d. **Termination Process:**
 - i. Upon occurrence of an event of default as set out in above clauses, NICS I will deliver a default notice in writing to the other party which shall specify the event of default and give the Empanelled agency an opportunity to correct the default.
 - ii. At the expiry of notice period, unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the agreement.
- e. Payments for all satisfactorily completed services till the time of termination shall be made to the agency in the event of termination, except in cases of insolvency.
- f. On termination, the exit management and transition provisions as per the RFE will come into effect.

16.7. Force Majeure

If at any time, during the continuance of the work order, the performance in whole or in part by either party of any obligation under the selection is prevented or delayed by reasons beyond the control of a party such as war, hostility, acts of public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics quarantine restrictions, strikes, natural calamities, lockouts, acts of state or acts of God (hereinafter referred to as "events"), provided notice of happenings of any such event is duly endorsed by the appropriate authorities/ chamber of commerce in the country of the party giving notice, is given by party seeking concession to the other as soon as practicable, but within twenty-one (21) days from the date of occurrence and termination thereof, neither party shall, by reason of such event, be entitled to terminate the work order/

contract, nor shall either party have any claim for damages against the other in respect of such non-performance or delay in performance, and deliveries under the work order/ contract shall be resumed as soon as practicable after such event has come to an end or ceased to exist, provided further, that if the performance in whole or in part or any obligation under the selection is prevented or delayed by reason of any such event for a period exceeding sixty (60) days, NICS I may at its option, terminate the work order.

Neither Party shall be liable for any failure or delay in the performance of its obligations under the contract or Work Orders here under to the extent such failure or delay or both is caused, directly, without fault by such Party, by reason of such event. NICS I shall however, be responsible to pay the selected Agency for the services successfully rendered to the satisfaction of NICS I under the Work/ Purchase Orders issued pursuant to the contract.

16.8. Fraud and Corrupt Practices

- a. The bidder and their respective officers, employees, agents, and advisers shall always observe the highest standard of ethics during the selection process. Notwithstanding anything to the contrary contained in this RFE, NICS I shall reject a bid without being liable in any manner whatsoever to the bidder, if NICS I determines that the bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice (collectively the “prohibited practices”) in the selection process. In such an event, NICS I shall, without prejudice to its any other rights or remedies, forfeit and appropriate the bid security / performance security as mutually agreed genuine pre estimated compensation and damages payable to NICS I for, inter alia, time, cost, and effort of NICS I, regarding the RFE, including consideration and evaluation of such bidder’s bid.
- b. Without prejudice to the rights of NICS I under the above sections other clauses and the rights and remedies which NICS I may have under the Letter of Intent (or the contract/ work order, if a bidder is found by NICS I to have directly or indirectly or through an agent, engaged or indulged in any prohibited practices during the selection process, or after the issue of the Lol or the execution of the contract/ work order, such bidders shall not be eligible to participate in any tender or RFE issued by NICS I for a minimum period of 3 years from the date such bidder is found by NICS I to have directly or through an agent, engaged or indulged in any prohibited practices, as the case may be.
- c. For the purposes of this section, the following terms shall have the meaning hereinafter respectively assigned to them:

“Corrupt practice” means

- the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the selection process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of NICS I who is or has been associated in any manner, directly or indirectly with the selection process before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of NICS I, shall be deemed to constitute influencing the actions of a person connected with the selection process); or
- engaging in any manner whatsoever, whether during the selection process or after the execution of the contract/ work order any person in respect of any matter relating to the

project or the contract/ work order, who at any time has been or is a legal, financial, or technical consultant adviser of NICSI in relation to any matter concerning the project.

“Fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, to influence the selection process.

“Coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any person or property to influence any person’s participation or action in the selection process.

“Undesirable practice” means

- establishing contact with any person connected with or employed or engaged by NICSI with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the selection process; or
- having a conflict of interest

“Restrictive practice” means forming a cartel or arriving at any understanding or arrangement among bidders with the objective of restricting or manipulating a full and fair competition in the selection process.

16.9. Governing Law and Jurisdiction

The Parties agree that this Agreement shall be governed by and construed in accordance with the laws of India. Subject to the arbitration clause below, the courts in India, shall have exclusive jurisdiction over any dispute, suit, or proceeding arising out of or in connection with this Agreement. The Parties agree that no court or tribunal outside India shall have any jurisdiction to entertain any dispute or claim arising out of or in connection with this Agreement. The Parties expressly waive any right to bring or participate in any legal proceedings in any foreign jurisdiction.

16.10. Arbitration

- a. NICSI and the empanelled bidder / agency will make every effort to resolve amicably any dispute arising between them under or in connection with the agreement / empanelment / work order / purchase order etc.
- b. If any dispute could not be settled between the parties amicably, then such dispute shall be referred to arbitration.
- c. The authority to appoint arbitrator(s) shall be the India International Arbitration Centre (IIAC). The India International Arbitration Centre shall provide administrative services.
- d. The award of the arbitration, as the case may be, will be final and binding on both parties. Such arbitration in all respects will be governed by the provision of the Indian Arbitration and Conciliation Act, 1996 (amended up to date) and the Rules made there under.
- e. The arbitration proceedings will be held at India International Arbitration Centre (IIAC), New Delhi, India.

- f. The fee of the Arbitrator(s) and the administrative charges of IIAC shall be borne equally by the parties.

In addition, NICSI reserves its rights to deal with dispute resolution as per OM No. F 1/2/2024-PPD dated 03/06/2024 issued by Government of India, Ministry of Finance, Department of Expenditure, Procurement Policy Division or any subsequent modifications made from time to time in this regard.

16.11. Conciliation

If a dispute arises out of or in connection with this contract, or in respect of any defined legal relationship associated therewith or derived there from, the parties agree to seek an amicable settlement of that dispute by Conciliation under the ICADR Conciliation Rules, 1996.

The Authority to appoint the Conciliator(s) shall be the International Centre for Alternative Dispute Resolution (ICADR).

The International Centre for Alternative Dispute Resolution will provide administrative services in accordance with the ICADR Conciliation Rules, 1996.

16.12. Applicable Law

The contract/ work-order(s) will be governed by the laws & procedures established by the Government of India within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/ processing. All disputes in this connection shall be settled in Delhi jurisdiction only.

16.13. Non-Solicitation

The Empanelled agency and NICSI/User department each agree that during the term, Empanelled agency personnel or NICSI/User department employee is associated with the services under the Contract and for a period of twelve months after such person ceases to be so associated, neither the Empanelled agency nor NICSI/User department shall, directly or indirectly, solicit for hire or knowingly hire or retain such personnel of the other party as an employee or independent contractor, except with prior written consent of the other party.

16.14. Confidentiality

- a. The selected Agency and its Personnel will not, either during the term or after expiration of this contract, disclose any proprietary or confidential information relating to the services, contract or business or operations of NICSI/User department without the prior written consent of NICSI/User department.
- b. The selected Agency will ensure that no information about the software/ hardware/ policies of NICSI/User department etc., is taken out in any form including electronic form or otherwise, by the manpower deployed by them.
- c. Additionally, the selected Agency shall keep all the details and information confidential with regards to the projects, including systems, facilities, operations, management, and maintenance of the systems/ facilities.

- d. NICSI/User department shall retain all rights to prevent, stop and if required take the necessary punitive action against the selected Agency regarding any forbidden disclosure.
- e. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:
 - i. Information already available in the public domain.
 - ii. Information which has been developed independently by the selected Agency.
 - iii. Information received from a third party who had the right to disclose the aforesaid information.
 - iv. Information which has been disclosed to the public pursuant to a court order.
 - v. Information required to be disclosed pursuant to an applicable law, rule, regulation, government requirement or court order, or the rules of any stock exchange (provided, however, that the Agency shall advise NICSI/User department of such required disclosure promptly upon learning thereof in order to afford NICSI/User department a reasonable opportunity to contest, limit and/or assist the Agency in crafting such disclosure).
- f. Any handover of the confidential information needs to be maintained in a list, containing at the very minimum, the name of the providers, recipients, dates of generation and handing over of the data, modes of information, purposes, and signatures of both the parties.
- g. Notwithstanding anything to the contrary mentioned hereinabove, the selected Agency shall have the right to share the Letter of Intent/ Work Order provided to it by NICSI in relation to this Agreement, with its prospective purchasers solely for the purpose of and with the intent to evidence and support of its work experience under this agreement.
- h. The obligations under this clause shall survive for three years from termination or expiration of this Contract.
- i. The work order/contract with the user department may define more stringent confidentiality obligations depending on the nature of information / data being shared. In such event, the more stringent obligations shall prevail.

16.15. Intellectual Property Rights (IPR)

Subject to the other provisions contained in this Clause, the Empanelled Agency shall agree that all deliverables created or developed by the Empanelled Agency, specifically for the NICSI/User department, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre (hereafter NIC).

NICSI/User department shall acknowledge that:

- a. In performing services under the Contract, the Empanelled Agency may use Empanelled Agency's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by the Empanelled Agency prior to or independent of the services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the services hereunder, ("the Empanelled Agency's Pre-Existing IP").
- b. Notwithstanding anything to the contrary contained in the Contract, the Empanelled Agency shall continue to retain all the ownership, the rights title and interests on all the Empanelled Agency's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Empanelled Agency from using the Empanelled Agency's Pre-Existing IP in any manner.

- c. If any of the Empanelled Agency's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the Empanelled Agency hereby grants to the NICS/ User department a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple Categories, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.
- d. NIC being the owner of all the IPs created in the deliverables, except the Pre-Existing IPs of the Empanelled Agency used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer, share, deploy, develop, modify or any such act that the NICS/ User department may require or find necessary for its purpose. The IP rights of the /NIC shall indefinitely subsist or continue in all future derivatives of the deliverables.
- e. The Empanelled Agency shall have no claims whatsoever on the deliverables and all the IPs created in deliverables or in course of development of the applications except its Pre-Existing IPs for which it shall grant all authorizations to the NICS/ User department for use as detailed in the Clause (c) above.
- f. Except as specifically and to the extent permitted by the Empanelled Agency, the NICS/ User department will not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source code of the Agency's Pre-Existing IP, or separate Empanelled Agency's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.
- g. The NICS/ User department shall warrant that the materials provided by the NICS/ User department to Empanelled Agency for use during development or deployment of the application shall be duly owned or licensed by the NICS/ User department.

17. ANNEXURES

ANNEXURE 1: Pre-Qualification Criteria

1.1. Pre-Qualification Evaluation for CSP

NICSI shall open the technical bids and evaluate the bids with respect to the minimum eligibility criteria as tabulated below. The CSP shall submit self-assessed compliance to the eligibility criteria checklist as prescribed in this RFE. Bids not conforming to any of the minimum eligibility criteria shall be outrightly rejected. NICSI may ask CSP(s) for additional information to verify claims made in their eligibility document, at any point of time before opening of the technical bid.

Note: The CSP can only quote in either Category – Tier-1 or Tier-2 or Tier-3 as per Eligibility Criteria. If any CSP quotes in more than one Category, then all submissions will be rejected simultaneously.

- a) For services offered in Tier-1, CSP can submit the bid with only one MSP.
- b) For services offered in Tier-2, one CSP can submit the bid with maximum two MSPs.
- c) For services offered in Tier-3, one CSP can submit the bid with maximum three MSPs.

Each of the applicable Pre-Qualification conditions mentioned in this section is MANDATORY for empanelment of the Cloud Service Providers (CSPs) in the respective category -

- Table 1.1: Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)
- Table 1a: Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)
- Table 1b: Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)
- Table 1c: Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)

Table 1.1: Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)

Basic Requirement	Eligibility Criteria	Documents to be submitted
Legal Entity	CSP must be a Legal Entity i.e., a company incorporated under the Indian Companies Act, 2013 or any other previous company law as per Section 2 (20) of the Indian Companies Act, 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act AND Registered with the Income Tax (TAN/PAN) and GST (GSTN) Authorities in India with active status.	Certified by Authorized Signatory: 1. Copy of Certificate of Incorporation/ Registration issued by registrar of Company (RoC). 2. Copy of GST Registration Certificate issued to bidder. 3. Copy of TAN/PAN card of the bidder
Empanelment	The Cloud Service Offerings of CSP should be MeitY empanelled.	1. Valid MeitY empanelment certificate. 2. Copy of Authorised partner certificates from CSP, signed by authorized signatory. 3. Authorization letter from the proposed CSP for bid submission against this BID.

		4. Authorization for the person signing and submitting the Bid.
Net Worth	The Bidder should have positive Net Worth for the preceding Three (03) financial years (FY2021-22, FY2022-23, FY 2023-24).	Certificate from the Statutory Auditor / Chartered Accountant. (ANNEXURE-21)
Blacklisting	The Bidder should not be blacklisted/debarred/suspended/banned by any Ministry/ Department of State or Central Government/PSU on the last date of submission to this RFE.	Self-declaration on bidder's letterhead (as per format provided in ANNEXURE-12).
DC & DR Sites	The Data Centres and DR offered for services by the Bidder should be in India. DC and DR Sites shall be (i) at least 100 Km apart and (ii) in different seismic zones if one of them (DC/DR) are in zone 1 or 2.	Undertaking on bidder's letterhead mentioning details of DC and DR, distance etc. (ANNEXURE-18)
Certifications	The bidder must possess the following certifications valid as on bid submission date: a. ISO/IEC 20000-1:2018 b. ISO 9001:2015 c. ISO 27001:2022 d. ISO/IEC 27017:2015	A self-attested copy of valid certifications awarded to the firm by the concerned accreditation agency/ Organization.
Self-Service Cloud Portal	Availability of self-service cloud portal and Command Line interface where administrator can provision & scale cloud resources without requiring manual intervention of CSP including at least- Virtual machine, network, backup, disaster recovery replication, infrastructure as code, infrastructure & security monitoring.	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.
Security Service	CSP must have the following security services in cloud for- a. NextGen Firewall b. Web Application Firewall c. DDoS Protection d. Data Encryption at-rest and in-transit e. Automated Security Assessment f. Identity and Access Management - fine grained access control for access to cloud resources (Only the user with appropriate permissions and grants should have access to a specific resource and all access and changes carried out must be logged, should not be tampered with and must be auditable).	<ul style="list-style-type: none"> Self- Declaration on bidder's letterhead supported by copies of certifications from Certifying Authorities duly attested by Authorised Signatory of the CSP. Undertaking on CSP letterhead with link to public facing website having the service and functionality description. Demonstration to be given at the time of

		technical presentation.
Security, Network and Monitoring Service	The Bidder must be able to provide security, network and monitoring services including but not limited to Firewall, WAF, Messaging as a service, Encryption, Load Balancer, application performance management tools as their own service or through their marketplace and should be available on demand.	Undertaking from the bidder for the services or URL/screenshot of the services.
Data Residency	Bidder is required to certify that data either rest or in motion at all times – reside within the geographical boundaries of India.	Undertaking on the bidder's letterhead, duly signed by Authorized Signatory (ANNEXURE-18)
Cloud Connectivity	The Bidder should provide mechanisms to establish private connectivity between the cloud infrastructure provisioned in DC and DR, which should provide a more consistent network experience than internet- based connections with low latency.	Undertaking from the bidder for the services or URL/screenshot of the services.
Data Migration experience	The Bidder must have proven data migration experience and capabilities, having successfully migrated a minimum of 1TB of data (within India) under a single contract order in the last three financial years.	The work order along with completion certificate must be submitted as per the documentary evidence.
Maintenance of KYC Information of Customers	The Bidder must submit the undertaking for maintaining the KYC of their customers as per guidelines of CERT-IN/other government agencies issued from time to time, periodically to NICS.	Undertaking from the Bidder as per ANNEXURE-17

Table 1a: Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted
Turnover	The CSP shall have an annual average turnover of INR 100 Cr from cloud business in the last 3 financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24).	Copy of the audited balance sheet for the last three financial years. In case of accounts not finalized for FY 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/ practising CA, mentioning business from Cloud Services. (ANNEXURE-22)
Manpower	The CSP should have a minimum 30 certified cloud resources on the proposed cloud platform on their payroll. The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid.	Certified by Company Secretary/ HR along with valid CSP certification along with certificate types. (ANNEXURE-10)
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: <ul style="list-style-type: none"> a. ISO/IEC 27018:2019 b. Service and Organization Controls (SOC) 1 c. Service and Organization Controls (SOC) 2 	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.
Managed Databases Features	CSP must have availability of databases having features of HA architecture & backup for industry standard databases.	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.
List of Cloud Services (Indicative)	List of basic cloud services essential for infrastructure management and operational efficiency including but not limited to: <ul style="list-style-type: none"> • Compute Services: Virtual Machines (VMs) & Auto-Scaling Instances 	Undertaking on CSP's letterhead with link to public facing website having the service

	<ul style="list-style-type: none"> • Storage Services: Object Storage, Block Storage, Archival Storage & Backup Solutions • Network Services: Virtual Private Cloud (VPC), Load Balancers & VPNs (Virtual Private Networks) • Database Services: Relational Databases, NoSQL Databases & In-Memory Databases • Security Services: Identity and Access Management (IAM) & Firewalls • Support Services: 24/7 Technical Support, Monitoring & Incident Management 	and functionality description.
Experience	<p>The CSP/MSP should have provisioned cloud services in India for at least Five (05) projects for a value not less than INR 10 Cr each</p> <p>OR</p> <p>at least Three (03) project of value not less than INR 20 Cr in the last 5 years from the last date of bid submission.</p>	<p>Copy of the Purchase order or Letter of Award or Contract of the work.</p> <p>Along with Proof of payments/ Invoices spanning over minimum 12 months.</p> <p>(ANNEXURE-11)</p>

Table 1b: Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted
Turnover	The CSP shall have an annual turnover of an average INR 500 Cr from cloud business in the last 3 (three) financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24).	Copy of the audited balance sheet for the last three financial years. In case of accounts not finalized yet for the year 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/practising CA, mentioning business from Cloud Services. (ANNEXURE-22)
Manpower	<p>The bidder should have a minimum 200 certified cloud resources on the proposed cloud platform on their payroll.</p> <p>The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid.</p>	Certified by Company Secretary/ HR along with valid CSP certification along with certificate

		types. (ANNEXURE-10)
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: a. ISO/IEC 27018:2019 b. Service and Organization Controls (SOC) 1 c. Service and Organization Controls (SOC) 2	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.
Managed Databases Features	CSP must have availability of managed databases (PaaS) having features of inbuilt scaling, HA architecture & backup for industry standard databases.	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.
List of Cloud Services (Tier-I + II)	<p>Services that offer essential and more advanced functionalities compared to the basic services but are not as specialized as the advanced services including but not limited to:</p> <ul style="list-style-type: none"> • Managed Database as a Service: A fully managed cloud database service offering automatic backups, scaling, and high availability without managing infrastructure. • Object Storage: Scalable cloud storage for unstructured data like media files and backups. • File Storage: Cloud storage providing network-attached file systems for shared access across multiple machines. • Native Network Services- VPN Gateway, Public IP & Web Application Firewall (WAF), DN service available in India. • Native Security Services- Cloud Security Posture Management (CSPM), IPDS (Intrusion Prevention and Detection Services) • Monitoring Services- Log Monitoring / Capturing, Operational Metric Collection, Alarm Service & Notification Service • Dedicated CSP Support for Large and Critical Applications: Provides 24/7 expert support for large-scale and mission-critical applications in the cloud. 	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.

Experience	The CSP/MSP should have provisioned cloud services in India for at least Four (04) projects for a value not less than INR 40 Cr each OR at least Two (02) project of value not less than INR 80 Cr each in the last 5 years from the last date of bid submission.	Copy of the Purchase order or Letter of Award or Contract of the work, along with Proof of payments/ Invoices spanning over minimum 12 months. (ANNEXURE-11)
-------------------	---	---

Table 1c: Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted
Turnover	The Bidder should have an annual turnover of an average INR 1000 Cr from cloud business in the last 3 financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24)	Copy of the audited balance sheet for the last three years is given. In case of accounts not finalized yet for the year 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/practising CA, mentioning business from Cloud Services. (ANNEXURE-22)
Manpower	The bidder should have a minimum 300 certified cloud resources on the proposed cloud platform on their payroll. The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid	Certified by Company Secretary/ HR along with valid CSP certification along with certificate types. (ANNEXURE-10)
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: <ul style="list-style-type: none"> a. ISO/IEC 27018:2019 b. ISO-22301:2019 c. Service and Organization Controls (SOC) 1 d. Service and Organization Controls (SOC) 2 	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.

Managed Databases Features	CSP must have availability of managed databases (PaaS) having features of inbuilt scaling, Multi -AZs HA architecture & backup for industry standard databases.	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.
List of Cloud Services (Tier-I + II+III)	<p>This category includes specialized and value-added cloud services, including but not limited to:</p> <ul style="list-style-type: none"> • Container Services: Kubernetes-based container orchestration and management. • Managed Database as a Service: Fully managed database services with backup and high availability. • Native Content Delivery Network (CDN): Global content distribution for optimized performance. • Native Security Services: <ul style="list-style-type: none"> • Hardware Security Module (HSM): Dedicated encryption key management services. • DDoS Protection: Enhanced security measures to mitigate cyber threats. • TLS/SSL Certificate Management: Centralized certificate lifecycle management. • Dual/Multi-Factor Authentication: Advanced authentication mechanisms. • Cloud-Native Security Services: SIEM/SOAR, threat protection (cloud workload), etc. • Monitoring Services: Real-time performance and security monitoring. • Native Analytics & AI/ML Services: <ul style="list-style-type: none"> • Analytics Services: AI/ML-enabled analytics, big data processing, and business intelligence. • CSP Managed DevOps Services: Automated DevOps solutions managed by CSPs. • CSP Managed Generative AI Services: AI-driven automation and content generation solutions. 	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.
Managing of Databases	The bidder should have Managed cloud native enterprise database services for MS-SQL EE, MS-SQL Std., MySQL and PostgreSQL. Similar service experience with value of 50 Cr.	Undertaking by both CSP and MSP on bidder's letterhead with link to public facing website having the service

		and functionality description.
Native Advance Services	<ul style="list-style-type: none"> • N/W Security • AIML • LLM • Other advance cloud services. 	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.
Experience	The CSP/MSP should have provisioned cloud services in India for at least Four (04) projects for a value not less than INR 200 Cr each OR at least Two (02) project of value not less than INR 400 Cr each in the last 5 years from the last date of bid submission.	Copy of the Purchase order or Letter of Award or Contract of the work, along with Proof of payments/ Invoices spanning over minimum 12 months. (ANNEXURE-11)

1.2. Pre-Qualification Evaluation for MSP

The MSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFE. NICSI will review the technical bids of the MSP to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at NICSI's discretion.

One MSP can only be authorized by only one CSP under either Category – Tier-1 or Tier-2 or Tier-3 as per Eligibility Criteria. Same MSP cannot be authorized by multiple CSP. If any MSP is authorized by multiple CSPs, then all submissions will be rejected simultaneously.

Each of the applicable Pre-Qualification conditions mentioned in this section is MANDATORY for NICSI empanelment of the Managed Service Providers (MSPs) in the respective category -

Table 1.1: Pre-Qualification Criteria (applicable for all categories - Tier-1 or Tier-2 or Tier-3)

Table 1a: Pre-Qualification Criteria for MSP in Tier-1 (Basic)

Table 1b: Pre-Qualification Criteria for MSP in Tier-2 (Intermediate)

Table 1c: Pre-Qualification Criteria for MSP in Tier-3 (Advanced)

Table 1.1: Pre-Qualification Criteria (applicable for all categories - Tier-1 or Tier-2 or Tier-3)

Sno.	Eligibility Criteria	Document to be submitted
1	The MSP should be an authorized partner of proposed MeitY empanelled CSPs.	Copy of Authorised partner certificates from CSP, signed by authorized signatory.
2	The MSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 and in operation for at least 5 years as on 31.03.2025. Consortium or JV not allowed.	Copy of Certificate of Incorporation/Registration/ Partnership deed

Sno.	Eligibility Criteria	Document to be submitted
3	The MSP must have a local office in India	Copy of address proof
4	The MSP must have a positive Net Worth in each of the three FY i.e. FY 21-22, FY 22-23 & FY 23-24 as per last audited financial report.	Certificate from the Statutory Auditor/ Chartered Accountant (ANNEXURE-21)
5	The MSP should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	Letter signed by the Authorized signatory in the format given in the RFE (ANNEXURE-12)
6	The bidder should not be subjected to any legal action for any cause in any legal jurisdiction in the last five years.	Letter signed by the Authorized (ANNEXURE-19)
7	The MSP should provide department the flexibility to create resources like Virtual instance, storage and other services of any configuration and should not restrict to specific configuration.	Letter from Authorized signatory on the letter head of the MSP
8	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal
9	The platform must offer a fully managed API management solution that enables secure API publishing, supports multi-cloud deployment, and provides advanced scalability features. The solution should be flexible and capable of integrating with a wide range of internal and external API consumers.	URL of the service on the MSP through portal

Table 1a: Pre-Qualification Criteria for MSP in Tier-1 (Basic Cloud Services)

S.No	Eligibility Criteria	Document to be submitted
1	The MSP should have average annual turnover of at least 50 Crore from IT/ITES business in last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant (ANNEXURE-22)
2	<p>Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central government/PSUs/Public Listed company in India within the last five years as per below:-</p> <ul style="list-style-type: none"> Five purchase orders each costing not less than the amount equal to Rs 6 Crores OR Two purchase orders each costing not less than the amount equal to Rs. 15 Crores OR 	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)

S.No	Eligibility Criteria	Document to be submitted
	<ul style="list-style-type: none"> One purchase orders each costing not less than the amount equal to Rs. 30 Crores <p>And bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 6 Crores within the last five years.</p>	
3	<p>The MSP must have strength of at least 30 IT Professionals (Data Centre / networking / system administration / cloud services professional's / cloud security experts etc.) on their payroll.</p> <p>a. The MSP should have minimum 6 certified cloud resources out of the above mentioned 30 resources on their payroll These certified cloud resources should be on Bidder's payroll for 6 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy. (ANNEXURE-10)</p>
4	<p>The MSP should have at least 3 certification out of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). ISO 20000-1 (IT service management systems certification, ensuring that the MSP follows best practices in IT service management). ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 	<p>Valid Copy of the Certificate to be attached.</p>
5	<p>The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its</p>	<p>URL of the service on the MSP through portal</p>

S.No	Eligibility Criteria	Document to be submitted
	flexibility and scalability for cloud infrastructure, data protection, and security use cases.	
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self-provisioning based on the Custom vCPU and RAM - Single Instance SLA: >= 99.5%</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM)</p>	URL of the service on the MSP through portal
7	The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine.	URL of the service through portal
8	<p>The proposed Cloud platform should have security services –</p> <p>The proposed cloud platform should provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, Continuous virtual red teaming including attack paths, risk scoring and toxic combinations.</p>	URL of the service through portal
9	The platform should offer managed database services for MySQL and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication. The solution must be flexible and compatible with industry standards for database management.	URL of the service through portal

Table 1b: Pre-Qualification Criteria for MSP in Tier-2 (Intermediate Cloud Services)

S.No	Eligibility Criteria	Document to be submitted
1	The MSP should have average annual turnover of at least 100 Crore from IT/ITES business in last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant (ANNEXURE-22)
2	<p>Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central government/PSUs/Public Listed company in India within the last five years as per below:-</p> <ul style="list-style-type: none"> Five purchase orders each costing not less than the amount equal to Rs 8 Crores OR Two purchase orders each costing not less than the amount equal to Rs. 20 Crores 	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)

S.No	Eligibility Criteria	Document to be submitted
	<p>OR</p> <ul style="list-style-type: none"> One purchase orders each costing not less than the amount equal to Rs. 40 Crores <p>And bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 8 Crores within the last five years.</p>	
3	<p>The MSP must have strength of at least 40 IT Professionals (Data Centre / networking / system administration / cloud services professional's / cloud security experts etc.) on their payroll.</p> <p>a. The MSP should have minimum 8 certified cloud resources out of the above mentioned 40 resources on their payroll These certified cloud resources should be on Bidder's payroll for 6 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy. (ANNEXURE-10)</p>
4	<p>The MSP should have at least 3 certification out of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). ISO 20000-1 (IT service management systems certification, ensuring that the MSP follows best practices in IT service management). ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 	<p>Valid Copy of the Certificate to be attached.</p>
5	<p>The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its</p>	<p>URL of the service on the MSP through portal</p>

S.No	Eligibility Criteria	Document to be submitted
	flexibility and scalability for cloud infrastructure, data protection, and security use cases.	
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self-provisioning based on the Custom vCPU and RAM - Single Instance SLA: >= 99.5%</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM).</p>	URL of the service on the MSP through portal
7	The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine.	URL of the service on the MSP through portal
8	<p>The proposed Cloud should have security services-</p> <ul style="list-style-type: none"> i. The proposed cloud platform must provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, and a customizable SIEM solution. These security services must be adaptable to multi-cloud environments. ii. Continuous virtual red teaming including attack paths, risk scoring and toxic combinations. iii. Cloud security and risk management for multi-cloud environments Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing for multi-cloud. 	URL of the service on the MSP through portal
9	The platform should offer managed database services for MySQL and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication. The solution must be flexible and compatible with industry standards for database management.	URL of the service on the MSP through portal

Table 1c: Pre-Qualification Criteria for MSP in Tier-3 (Advanced Cloud Services)

S. No	Eligibility Criteria	Document to be submitted
1	The MSP should have an average annual turnover of at least 200 Crore from IT/ITES business in the last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/ Chartered Accountant (ANNEXURE-22)
2	Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)

S. No	Eligibility Criteria	Document to be submitted
	<p>government/PSUs/Public Listed company in India within the last five years as per below:-</p> <ul style="list-style-type: none"> • Five purchase orders each costing not less than the amount equal to Rs 10 Crores OR • Two purchase orders each costing not less than the amount equal to Rs. 25 Crores OR • One purchase orders each costing not less than the amount equal to Rs. 50 Crores <p>And the bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 10 Crores within the last five years.</p>	
3	<p>The MSP must have strength of at least 50 IT Professionals (Data Centre / networking / system administration / cloud services professionals / cloud security experts etc.) on their payroll. The MSP should have minimum 30 certified cloud resources of the proposed cloud platform out of the above mentioned on their payroll These certified cloud resources should be on Bidder's payroll for 3 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy (ANNEXURE-10)</p>
4	<p>The MSP must have at least three of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ▪ ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ▪ ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). ▪ ISO 20000-1 (IT service management systems certification, ensuring that the MSP follows best practices in IT service management). ▪ ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ▪ ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). 	<p>Valid Copy of the Certificate to be attached.</p>

S. No	Eligibility Criteria	Document to be submitted
	<ul style="list-style-type: none"> ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 	
5	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self-provisioning based on the Custom vCPU and RAM - Single Instance SLA: $\geq 99.5\%$</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM) and support serverless data lake services with integration capabilities for advanced analytics, including machine learning (ML) and generative AI models. The platform should meet industry-standard SLAs.</p>	URL of the service on the MSP through portal
7	<p>The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine.</p> <p>The cloud platform should support scalable storage with low-latency performance, allow for on-demand scaling without requiring virtual machine reboots, and ensure resilience across multiple availability zones (AZs) or regions. The solution should be flexible and compatible with industry-standard storage protocols.</p>	URL of the service on the MSP through portal
8	<p>The proposed Cloud should have security services-</p> <ol style="list-style-type: none"> The proposed cloud platform must provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, and a customizable SIEM solution. These security services must be adaptable to multi-cloud environments. Continuous virtual red teaming including attack paths, risk scoring and toxic combinations. Cloud security and risk management for multi-cloud environments Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing for multi-cloud. 	URL of the service on the MSP through portal
9	The cloud platform should support a variety of AI/ML models for tasks such as text generation, summarization, and chatbots, irrespective of whether they are proprietary or open-source. The platform should provide an ecosystem that facilitates seamless	URL of the service on the MSP through portal or Demonstrate during the Presentation

S. No	Eligibility Criteria	Document to be submitted
	integration and deployment of different AI models for various use cases.	
10	The platform should offer CSP Native managed database services for MySQL, MS SQL EE and standard and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication across multiple availability zones or regions. The solution must be flexible and compatible with industry standards for database management.	URL of the service on the MSP through portal
11	<p>The MSP should have Unified End-to-End AI/ML Platform as Managed service that focus on MLOps & LLMOps principles which includes:</p> <ol style="list-style-type: none"> The platform should provide a comprehensive, end-to-end AI/ML solution that includes capabilities for model training, versioning, orchestration, and deployment at scale. The platform should also support AI-powered language translation services for a variety of languages, including regional Indian languages, with flexible deployment options. Flexible model serving options (online or batch prediction) at scale with optimized infrastructure. Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving. Platform must provide flexibility to deploy model on a private endpoint and also to be able to export a model to make it portable, like running in a container. Language translation service in speech to speech, speech to text, text to speech and text to text for Indian languages. 	URL of the service on the MSP through portal
12	The platform must offer a fully managed API management solution that enables secure API publishing, supports multi-cloud deployment, and provides advanced scalability features. The solution should be flexible and capable of integrating with a wide range of internal and external API consumers	URL of the service on the MSP through portal

ANNEXURE 2: Technical Evaluation Criteria

2.1. Technical Evaluation Criteria for CSPs:

- a) Technical proposals will be evaluated for those bidders who meet the pre-qualification criteria (PQC).
- b) The NICSI will evaluate the Technical Proposals based on the Technical Qualification criteria (TQC) for Proposed CSP and the supporting documents/forms as detailed in the below sections. Technical proposals must be supported by appropriate documents as outlined in [ANNEXURE-8](#) (Technical Qualification Proposal Format).
- c) Bid should be complete in all aspects covering the entire scope of work and should completely fulfil the technical specifications indicated in the bid document. Incomplete bids may face rejection or reduced evaluation scores.
- d) Bidder shall be responsible for providing Cloud services for entire bouquet of services from the proposed CSP as per Category
- e) Bidder shall Submit documentary proof for POC (Proof of Capability), as part of technical evaluation, to demonstrate its understanding of the key features such as AUTO Scale up/down, Security protocols, Denial of Service (DoS, DDoS attack), management and administration and audit capabilities of offerings, setting up of DR facilities, etc. The bidder may be asked to demonstrate any/all the services during the presentation.
- f) NICSI will evaluate the Technical Proposals of the bidders to determine whether the Technical Proposals are substantially responsive. Proposals of Bidders that are not substantially responsive are liable to be disqualified by NICSI.
- g) Each bidder, whose Technical Proposal is determined to be substantially responsive, would then be assigned technical score (referred as TS) based on the criteria set forth in the Tables below. The scoring will be transparent and based on compliance and functionality as outlined in the criteria.
- h) Bidders who fulfil all the technical compliance for Specific CSP and secure a minimum of 70 marks out of 100 marks in the Technical Qualification Criteria (TQC) would be declared as Technically qualified and shall qualify for financial / commercial evaluation.

Table 2.1.a: Technical Qualification Criteria (TQC) - Basic Cloud Services

S.No	Requirements	Max Marks	Criteria
1	All the services should be available from the India Region of the Cloud Service Provider (CSP). CSP should follow the guidelines from MeitY and ensure that all Data and the services used should remain in India.	15	Valid copy of the MeitY certificate
2	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1 & SOC 2. The bidder must provide valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.	15	Valid copy of the MeitY certificate Valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.
3	The Cloud Service Offerings of CSP should be MeitY empanelled & STQC audited as per MeitY empanelment	15	Valid copy of the MeitY certificate

	process as on the last date of submission of the bid.		
4	The CSP must be operating at least two (2) Data Centre / Disaster Recovery Centre Facilities in India located in different seismic zones from the DC, to withstand natural disasters with proven disaster recovery (DR) procedures, including regular testing of failover mechanisms.	25	Valid copy of the Meity certificate
5	SLA for its cloud services: - Service Level Agreements (SLA's) for its cloud services - Dashboard with real time service health for all its cloud services across all data centres. Service Level Agreements (SLAs) should guarantee 99.5% uptime and clear timelines for issue resolution. The service health dashboard must be accessible and updated in real-time.	10	CSP Link or Demonstration
6	Evaluate the ease of provisioning agility, self-service availability of different configurations of VM's for self-provisioning - Service console for provisioning and management of services like server configurations (CPU, memory, storage) - Available offerings/resources: Storage capabilities, Compute capabilities, Database capabilities and types, Networking and Other capabilities Bidders must demonstrate ease of provisioning with self-service availability of VMs, auto-scaling options, and seamless integration with other services.	10	CSP Link or Demonstration
7	Different types of available storage (e.g. block, object, and file) and data lifecycle process - Establish storage volume and demonstrate/Show how data is loaded and retrieved - Permissions and access management of the volumes The bidder should provide demonstrations of available storage	10	CSP Link or Demonstration

	types (block, object, file), with proof of redundancy, failover mechanisms, and access controls for each storage type.		
TOTAL		100	

Table 2.1.b: Technical Qualification Criteria (TQC) - Intermediate Cloud Services

S.No	Evaluation Criteria	Max Marks	Criteria
1	<p>The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles.</p> <p>The bidder must provide valid, up-to-date copies of SOC 1, SOC 2 certificates for the last audit cycle.</p>	2	Valid copy of the certificate
2	<p>The CSP should have the following certifications valid as on bid submission date:</p> <p>a. ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards.</p> <p>b. ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.</p> <p>c. ISO/IEC 20000-9 - Guidance on the application of ISO/IEC 20000-1 to cloud services.</p>	5	Valid copy of the certificate
3	<p>The CSP should provide different options like PAYG, 1-year commit and 3-year commit compute infrastructure and Public pricing/calculator for the price validation and verification.</p> <p>Provide detailed pricing models, including options for PAYG, 1-year, and 3-year commitment plans, with breakdowns of the cost per service</p>	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation
4	<p>The CSP data lake platform should have End-to-end ML using SQL applications building on the same platform to save the deployment cycle, effort and cost with SLA of 99.5% to enhance the reliability and user experience with capabilities of GenAI Integration and inbuilt Machine learning models.</p>	5	URL of the service on the CSP Product Page
5	<p>The CSP should have managed security services-</p>	5	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> a. WAF & DDoS Protection with enterprise features such as Threat Intelligence, Third-party named IP address & Adaptive Protection b. Threat detection, Vulnerability Assessment, Bot management with captcha Integration c. Cloud Native Security services – IPDS d. Continuous virtual red teaming including attack paths, risk scoring, and toxic combinations, e. Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing 		
6	The CSP should have State-of-the-art multi-modal LLMs for Text Generation, Summarization, Chatbots and Conversational with deployable options on the CSP managed AI/ML Platform.	7	Public Links and Letter from Authorized signatory on the letter head of the bidder.
7	<p>The CSP should have Managed cloud native enterprise database services for MySQL and PostgreSQL with the following features:</p> <ul style="list-style-type: none"> a. Enterprise Database services with 99.5% SLA b. Automated backups and point-in-time recovery or equivalent c. Automatic Storage Increase d. Automated replication / Automatic failover to another Zone e. HA architecture with Sync/async replication 	10	Public Links and Letter from Authorized signatory on the letter head of the bidder.
8	<p>The CSP should have Managed cloud Kubernetes service with the following features:</p> <ul style="list-style-type: none"> a. Secure Verified Container Images for software supply-chain security b. Container Threat Detection as inbuilt service with Dashboard c. Vertical/Horizontal Pod Autoscaler and Node auto-upgrades 	5	Public Links and Letter from Authorized signatory on the letter head of the bidder.
9	<p>The CSP must have GPU based machines with unified End-to-End AI/ML Platform as Managed service as one of the publicly listed services. The minimum Technical Specifications of GPUs:</p> <ul style="list-style-type: none"> a. FP32 - 30.3 tera FLOPs or above configuration b. GPU Memory- 24 GB or above configuration 	2	Public Links and Letter from Authorized signatory on the letter head of the bidder.
10	The CSP should have centralized security solution providing a single, consolidated view	2	URL of the service on the CSP

	of the organization security posture covering the following features: <ul style="list-style-type: none"> • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring • Risk Prioritization • Incident Response • Discovery and Inventory 		through Self provisioning portal
11	The CSP should have the CDN service.	5	URL of the service on the CSP Product Page/Marketplace
12	The CSP should have Managed cloud Auto-Scaling capabilities with the following features: <ul style="list-style-type: none"> - Predictive autoscaling by forecasting future load & scaling out in advance or equivalent - Schedule-based autoscaling - Utilization metrics based autoscaling The bidder should demonstrate their auto-scaling capabilities, including predictive scaling based on load forecasts, and provide case studies or performance metrics to validate the effectiveness or the bidder needs to set threshold for CPU and RAM, to achieve autoscaling with desired performance	2	URL of the service on the CSP Product Page
13	The CSP Should have Managed Object storage service with the following features: <ul style="list-style-type: none"> - Object's lifecycle by using a lifecycle configuration - Support read-after-write consistency for addition of any object - No minimum billable object size - Data Exfiltration control - Default data encryption at rest - Ability to charge requester for data retrieval cost 	7	URL of the service on the CSP Product Page
14	The CSP should have Managed cloud NoSQL database services with the following features <ul style="list-style-type: none"> -Serverless NoSQL key value pair document DB -Automated replication to different zones/geo-resilient data centres. -Encryption at rest -Fully managed with no planned downtime 	2	URL of the service on the CSP Product Page
15	The CSP Should support the Managed Hadoop Service	2	URL of the service on the CSP Product Page
16	The CSP should have Managed Security Services with following features:	7	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> -Web Application Firewall supporting TOP 10 OWASP -DDoS Protection -Threat detection, Vulnerability Assessment, -Identity and Access Management - fine grained access control for access to cloud resources -Single Sign-On & Multi factor Authentication - Cloud HSM & Key Mgmt. - Password Management -SSL Certificate -Discover, classify, and protect data using native Data Loss Prevention -Real-time log management and analysis -Identity and context to guard the access of VMs and Applications 		
17	<p>The CSP should have Managed Backup & DR Service with following features:</p> <ul style="list-style-type: none"> -Instant mount and recovery -Application-consistent backups -Application-aware backup and recovery for databases 	5	URL of the service on the CSP Product Page
18	<p>The CSP should have the following managed networking services:</p> <ul style="list-style-type: none"> - IPv4, IPv6 - DHCP - IPSec VPN Tunnel Creation - Geo/Network load Balance (Balancing between multiple sites) - Load Balancer. (Internal and External Load Balancers) - L3 and L4 Anti-DDoS solution 	2	URL of the service on the CSP Product Page
19	<p>Details Demo and Presentation of Database as service Active/Standby and DR automatic replication, Kubernetes as services with sample application monitoring & Pods Scaling, Backup and DR configuration for MS-SQL Database running on VMs, GPUs Machines with flexibility to add/remove GPUs on demand etc.</p>	20	In-Person Demonstration of the required services
TOTAL		100	

Table 2.1.c: Technical Qualification Criteria (TQC) - Advanced Cloud Services:

S. No	Evaluation Criteria	Max Marks	Criteria
1	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. The bidder must provide valid, up-to-date copies of SOC 1, SOC 2 certificates for the last audit cycle.	2	Valid copy of the certificate
2	The CSP should have the following certifications valid as on bid submission date: <ul style="list-style-type: none"> a. ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards. b. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology. c. ISO 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds. d. ISO-22301 for Business Continuity Management. e. ISO/IEC 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services. f. ISO/IEC 42001:2023 - Information technology — Artificial intelligence — Management system 	5	Valid copy of the certificate
3	CSP should provide different options like PAYG, 1 year commit and 3 year commit compute infrastructure with different list pricing per selection e.g. On-Demand, 1, 3 years etc. and Public pricing/calculator for the price validation and verification.	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation
4	The CSP data lake platform should have End-to-end ML using SQL applications building on the same platform to save the deployment cycle, effort and cost with SLA of 99.95% to enhance the reliability and user experience with capabilities of GenAI Integration and inbuilt Machine learning models.	5	URL of the service on the CSP Product Page
5	The CSP should have Native security services-	5	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> a. WAF & DDoS Protection with enterprise features such as Threat Intelligence, Third-party named IP address & Adaptive Protection b. Threat detection, Vulnerability Assessment, Bot management with captcha Integration c. Cloud Native Security services – IPDS d. Continuous virtual red teaming including attack paths, risk scoring, and toxic combinations e. Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing 		
6	CSP should have native State-of-the-art multi-modal LLMs for Text Generation, Summarization, Chatbots and Conversational with deployable options on the CSP native fully managed AI/ML Platform.	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation
7	<p>The CSP should have Managed cloud native enterprise database services for MS-SQL EE, MS-SQL Std., MySQL and PostgreSQL with the following features:</p> <ul style="list-style-type: none"> a. Enterprise Database services with synchronous replication and automatic failover of a primary database to a standby database copy in a separate physical data centre in the same region to ensure high availability and low latency. b. Automated backups and point-in-time recovery for database lifecycle management e.g. Provisioning, de-provisioning, patching, backups, DR configuration, HA etc. c. Automatic Storage Increase d. Redundant Zone High Availability (HA) architecture with automated replication and automatic failover to another availability zone. e. Redundant Zone HA architecture with self-service public APIs for managing database functions, including start/stop, backup, restoration, configuration, and scaling. 	10	URL of the service on the CSP Product Page
8	<p>The CSP should have native Unified End-to-End AI/ML Platform as Managed service that focus on MLOps & LLMOps principles which includes:</p> <ul style="list-style-type: none"> a. Managed services for Model training 	7	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> b. Build, orchestrate, and automate reproducible ML workflows, easing the transition from experimentation to production c. Centralized repository for managing, versioning, and tracking trained ML models d. Flexible model serving options (online or batch prediction) at scale with optimized infrastructure e. Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving f. Platform must provide flexibility to deploy model on a private endpoint and also to be able to export a model to make it portable, like running in a container" g. Language translation service in speech to speech, speech to text, text to speech and text to text for Indian languages. 		
9	<p>CSP must offer Kubernetes/Containerized environment that should have following capabilities from Day 1:</p> <ul style="list-style-type: none"> a. Capability for regional clusters to replicate cluster masters and nodes across multiple zones within a single region. b. Kubernetes resources are spread across multiple zones of a region c. K8S cluster must provide features to help keep the platform secure with automatic upgrades of the node OS and Kubernetes components via Automatic Node Upgrades. d. CSP should provide tools for application modernization like Native managed Kubernetes services and CSP Native CI/CD pipelines. e. Secure Verified Container Images for software supply-chain security 	5	URL of the service on the CSP Product Page
10	<p>The CSP must have GPU based machines with unified native End-to-End AI/ML Platform as Managed service as one of the publicly listed services. The minimum Technical Specifications of GPUs:</p> <ul style="list-style-type: none"> a. FP32 - 30.3 teraflops Or Above Configuration b. GPU Memory- 24 GB/GPU or Above Configuration 	2	Public Links and Letter from Authorized signatory on the letter head of the bidder.
11	<p>Centralized Security solution providing a single, consolidated view of the organization security posture covering the following features:</p> <ul style="list-style-type: none"> • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring 	2	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> • Risk Prioritization • Incident Response • Discovery and Inventory 		
12	The CSP should have Native CDN service with Compliances.	10	CSP Native Public Links and Letter from Authorized signatory on the letter head of the bidder.
13	<p>The CSP should have Managed Compute Services with the following features:</p> <ul style="list-style-type: none"> - Container Optimize O/S - Option to disable Simultaneous Multi-Threading (SMT) - Scheduler for Start and Pause to preserves the state of a VM on restart -CSP Native Linux Images like - RHEL, SUSE, Debian, Ubuntu with native billing for RHEL & SUSE. 	6	URL of the service on the CSP Product Page
14	<p>The CSP should have Managed cloud native Auto-Scaling capabilities with the following features:</p> <ul style="list-style-type: none"> - Predictive autoscaling by forecasting future load & scaling out in advance - Schedule-based autoscaling - Utilization metrics based autoscaling 	2	URL of the service on the CSP Product Page
15	The CSP should have the Managed cloud native Serverless computing	2	URL of the service on the CSP Product Page
16	<p>The CSP should have Managed Object storage service with the following features:</p> <ul style="list-style-type: none"> - Average sub millisecond retrieval time including archival tier - Object's lifecycle by using a lifecycle configuration - Support read-after-write consistency for addition of any object - No minimum billable object size - Data Exfiltration control - Default data encryption at rest - Ability to charge requester for data retrieval cost 	3	URL of the service on the CSP Product Page
17	<p>The CSP should have Managed cloud native NoSQL database services with the following features</p> <ul style="list-style-type: none"> -Serverless NoSQL key value pair document DB -Automated replication to different zones -Encryption at rest -Fully managed with no planned downtime 	1	URL of the service on the CSP Product Page
18	The CSP should support the Managed Hadoop Service	1	URL of the service on the CSP Product Page
19	<p>The CSP should have Managed Security Services with following features:</p> <ul style="list-style-type: none"> -Web Application Firewall supporting TOP 10 OWASP 	2	URL of the service on the CSP Product Page

	<ul style="list-style-type: none"> -DDoS Protection -Threat detection, Vulnerability Assessment, -Identity and Access Management - fine grained access control for access to cloud resources -Single Sign-On & Multi factor Authentication - Cloud HSM & Key Mgmt. - Password Management -SSL Certificate -Discover, classify, and protect data using native Data Loss Prevention -Real-time log management and analysis -Identity and context to guard the access of VMs and Applications 		
20	<p>The CSP should have Managed native Backup & DR Service with following features:</p> <ul style="list-style-type: none"> -Instant mount and recovery -Application-consistent backups -Application-aware backup and recovery for databases 	4	URL of the service on the CSP Product Page
21	<p>The CSP should have the following managed networking services:</p> <ul style="list-style-type: none"> - IPv4, IPv6 - DHCP - IPsec VPN Tunnel Creation - Geo load Balance (Balancing between multiple sites) - Load Balancer. (Internal and External Load Balancers) - L3 and L4 Anti-DDoS solution 	1	URL of the service on the CSP Product Page
22	<p>Details Demo and Presentation of CSP Native Auto-scaling, Compute Services with O/S Images of RHEL, SUSE native billing, Multi-Threading (SMT) of vCPUs, Consolidated view of the security posture, Native CDN integration with Cloud Services & Unified AI Platform with GPUs training options, CSP native MS-SQL EE. Database as service Active/Standby and DR automatic/inbuilt replication to different Regions/DCs.</p>	15	In-Person Demonstration of the required services
TOTAL		100	

ANNEXURE 3: COVERING LETTER

<To be submitted on the letterhead of the bidder>

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSII)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: Submission of Bid for RFE No.

Dear Sir,

This is to notify that our company is submitting technical bid in response to REF No <.....REF No.....> for <.....Name of the REF.....> for <.....Name of the Category.....> Primary & Secondary contact for our company are as follows:

<M/s Company Name>	Primary Contact	Secondary Contact
Name		
Title		
Address		
Phone		
Mobile		
Email		

We are responsible for communicating to the NICSII in case of any change in the Primary or/and Secondary contact information mentioned above. We shall not hold NICSII responsible for any non-receipt of bid process communication in case such change of information is not communicated and confirmed with NICSII on time.

We are submitting our bid for Empanelment under the category <Mention Category> for Provisioning of Cloud Services as per the scope and requirements of the REF document.

By submitting the proposal, we acknowledge that we have carefully read all the sections of this REF document including all forms, scheduled and appendices hereto, and are fully informed to all existing conditions and limitations. We also acknowledge that the company is in agreement with terms and conditions of the REF and the procedure for bidding and evaluation.

We agree to abide by this Application, consisting of this letter, with all the annexures, duly signed, valid for a period of 180 days from the submission date specified in this application document.

We have enclosed the earnest money deposit as per the REF Conditions. It is liable to be forfeited in accordance with the provisions of REF document.

Deviations:

We declare that all the services shall be performed strictly in compliance with the REF Document. Further, we agree additional conditions, if any, found in the bid documents, other than those stated in the REF document, shall not be given effect to.

Bid Pricing:

We do hereby confirm that our bid prices exclusive all taxes, as applicable on the last date of submission of bid. We further declare that the prices stated in our proposal are in accordance with your terms & conditions in the bidding document.

Qualifying Data:

We confirm having submitted in qualifying data as required by you in your REF document. In case you require any further information/documentary proof in this regard before evaluation of bid, we agree to furnish the same in time to your satisfaction.

We confirm that information contained in this response or any part thereof, including documents and instruments delivered or to be delivered to NICSI are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part misled NICSI in its evaluation process.

We fully understand and agree that on verification, if any of the information provided here is found to be misleading the evaluation process or result in unduly favours to our company in evaluation process, we are liable to be dismissed from the selection process or termination of the contract during the empanelment with NICSI.

We understand that you are not bound to accept the lowest or any bid you may receive.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 4: Format for Earnest Money Deposit (EMD)

[Date]

From:

Bank _____

To,

The Managing Director,

National Informatics Centre Services Incorporated (NICSI)

1st Floor, NBCC Tower,

Bhikaji Cama Place, New Delhi-110066.

1. In consideration of _____ (hereinafter called the "NICSI") represented by _____, on the first part and M/s _____ of _____ (hereinafter referred to as "Applicant") on the Second part, having agreed to accept the Earnest Money Deposit of Rs. _____ (Rupees _____) in the form of Bank Guarantee for the Application for Rate Empanelment of MSPs for Provisioning of Cloud Services, we _____ (Name of the Bank), (hereinafter referred to as the "Bank"), do hereby undertake to pay to the NICSI forthwith on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding _____ (Rupees _____) and the guarantee will remain valid up to a period of 180 days from the date of submission of application. It will, however, be open to the NICSI to return the Guarantee earlier than this period to the Applicant in case the applicant has been notified by the NICSI as being unsuccessful.

2. In the event of the successful application, if the applicant fails to acknowledge and accept the Letter of Award of Empanelment from NICSI in accordance with the terms and conditions of the Empanelment Application, the EMD deposited by the applicant stands forfeited to the Government. We also undertake not to revoke this guarantee during this period except with the previous consent of the Government in writing and we further agree that our liability under the EMD shall not be discharged by any variation in the term of the said REF and we shall be deemed to have agreed to any such variation.

3. No interest shall be payable by the NICSI to the Applicant on the guarantee for the period of its currency.

4. Notwithstanding anything contained hereinabove:

- a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs. _____ (Rupees _____ only)
- b) This Guarantee shall remain in force up to and including _____.
- c) Unless the demand/claim under this guarantee is served upon us in writing before _____ all the rights of NICSI under this guarantee shall stand automatically forfeited and we shall be relieved and discharged from all liabilities mentioned hereinabove.

Dated this _____ day of _____ Year

For the Bank of _____

(Agent/Manager)

ANNEXURE 5: Format for Bid Securing Declaration

<On Company's Letter Head>

Date: _____ REF No. _____

To *(insert complete name and address of the purchaser)*

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 three 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 REF, or defaults in respect to REF terms & conditions, my/our Bid during the period of bid validity specified in the form of Bid; or
- b. have quoted incredibly low or high value of items leading to subvert the REF process, or
- c. do not accept correction of the errors, if in case a discrepancy is found in our Financial Bid between the unit price and the total price; the unit price shall prevail, and the total price is corrected, or
- d. having been notified of the acceptance of our Bid by the purchaser during the period of bid validity
 - i. fail or reuse 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 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 he 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

ANNEXURE 6: Format for Power of Attorney / Bidder's Authorization Certificate

<On Company's Letter Head>

To,
The Managing Director,
National Informatics Centre Services Incorporated (NICS)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Ref: Bid No: <RFE Reference Number here> Dated <DD/MM/YYYY>

This is to certify that <Personnel Name>, <Designation> from <Bidder's Name> is hereby authorized to sign relevant documents on behalf of the Proprietorship/ Partnership firm/ Company in dealing with RFE of <RFE Reference Number here> dated <xx/xx/xxxx>.

He is also authorized to attend meetings and submit technical and commercial information as may be required by you in the course of processing above said RFE.

Yours Sincerely,

Signature of the Bidder with stamp

Name

Designation

Date

ANNEXURE 7: Form for Submission of Pre-qualification Information

7.1. Compliance Sheet for CSPs Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)

Basic Requirement	Eligibility Criteria	Documents to be submitted	Provided (Yes/No)	Reference Page No.
Legal Entity	CSP must be a Legal Entity i.e., a company incorporated under the Indian Companies Act, 2013 or any other previous company law as per Section 2 (20) of the Indian Companies Act, 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act AND Registered with the Income Tax (TAN/PAN) and GST (GSTN) Authorities in India with active status.	Certified by Authorized Signatory: 1. Copy of Certificate of Incorporation/ Registration issued by registrar of Company (RoC). 2. Copy of GST Registration Certificate issued to bidder. 3. Copy of TAN/PAN card of the bidder		
Empanelment	The Cloud Service Offerings of CSP should be MeitY empanelled.	1. Valid MeitY empanelment certificate. 2. Copy of Authorised partner certificates from CSP, signed by authorized signatory. 3. Authorization letter from the proposed CSP for bid submission against this BID. 4. Authorization for the person signing and submitting the Bid.		
Net Worth	The Bidder should have positive Net Worth for the preceding Three (03) financial years (FY2021-22, FY2022-23, FY 2023-24).	Certificate from the Statutory Auditor / Chartered Accountant. (ANNEXURE-21)		
Blacklisting	The Bidder should not be blacklisted/ debarred/suspended/banned by any Ministry/ Department of State or Central Government/PSU on the last date of submission to this RFE.	Self-declaration on bidder's letterhead (as per format provided in ANNEXURE-12 : Self-declaration for non-black listing).		
DC & DR Sites	The Data Centres and DR offered for services by the Bidder should be in India. DC and DR Sites shall be (iii) at least 100 Km apart and	Undertaking on bidder's letterhead mentioning details of DC and DR, distance etc. (ANNEXURE-18)		

	(iv) in different seismic zones if one of them (DC/DR) are in zone 1 or 2.			
Certifications	The bidder must possess the following certifications valid as on bid submission date: a. ISO/IEC 20000-1:2018 b. ISO 9001:2015 c. ISO 27001:2022 d. ISO/IEC 27017:2015	A self-attested copy of valid certifications awarded to the firm by the concerned accreditation agency/ Organization.		
Self-Service Cloud Portal	Availability of self-service cloud portal and Command Line interface where administrator can provision & scale cloud resources without requiring manual intervention of CSP including at least- Virtual machine, network, backup, disaster recovery replication, infrastructure as code, infrastructure & security monitoring.	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.		
Security Service	CSP must have the following security services in cloud for- a. NextGen Firewall b. Web Application Firewall c. DDoS Protection d. Data Encryption at-rest and in-transit e. Automated Security Assessment f. Identity and Access Management - fine grained access control for access to cloud resources (Only the user with appropriate permissions and grants should have access to a specific resource and all access and changes carried out must be logged, should not be tampered with and must be auditable).	<ul style="list-style-type: none"> • Self- Declaration on bidder's letterhead supported by copies of certifications from Certifying Authorities duly attested by Authorised Signatory of the CSP. • Undertaking on CSP letterhead with link to public facing website having the service and functionality description. • Demonstration to be given at the time of technical presentation. 	•	•
Security, Network and Monitoring Service	The Bidder must be able to provide security, network and monitoring services including but not limited to Firewall, WAF, Messaging as a service, Encryption, Load Balancer, application performance management tools as their own service or through their marketplace and should be available on demand.	Undertaking from the bidder for the services or URL/screenshot of the services.		

Data Residency	Bidder is required to certify that data either rest or in motion at all times – reside within the geographical boundaries of India.	Undertaking on the bidder's letterhead, duly signed by Authorized Signatory (ANNEXURE-18)		
Cloud Connectivity	The Bidder should provide mechanisms to establish private connectivity between the cloud infrastructure provisioned in DC and DR, which should provide a more consistent network experience than internet- based connections with low latency.	Undertaking from the bidder for the services or URL/screenshot of the services.		
Data Migration experience	The Bidder must have proven data migration experience and capabilities, having successfully migrated a minimum of 1TB of data (within India) under a single contract order in the last three financial years.	The work order along with completion certificate must be submitted as per the documentary evidence.		
Maintenance of KYC Information of Customers	The Bidder must submit the undertaking for maintaining the KYC of their customers as per guidelines of CERT-IN/other government agencies issued from time to time, periodically to NICSI.	Undertaking from the Bidder as per ANNEXURE-17		

7.2. Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted	Provided (Yes/No)	Reference Page No.
Turnover	The CSP shall have an annual average turnover of INR 100 Cr from cloud business in the last 3 financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24).	Copy of the audited balance sheet for the last three financial years. In case of accounts not finalized for FY 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/ practising CA, mentioning business from Cloud Services. (ANNEXURE-22)		
Manpower	The CSP should have a minimum 30 certified cloud resources on the proposed cloud platform on their payroll.	Certified by Company Secretary/ HR along with valid CSP certification		

	The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid.	and certificate types. (ANNEXURE-10)		
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: <ul style="list-style-type: none"> d. ISO/IEC 27018:2019 e. Service and Organization Controls (SOC) 1 f. Service and Organization Controls (SOC) 2 	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.		
Managed Databases Features	CSP must have availability of databases having features of HA architecture & backup for industry standard databases.	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.		
List of Cloud Services (Indicative)	<p>List of basic cloud services essential for infrastructure management and operational efficiency including but not limited to:</p> <ul style="list-style-type: none"> • Compute Services: Virtual Machines (VMs) & Auto-Scaling Instances • Storage Services: Object Storage, Block Storage, Archival Storage & Backup Solutions • Network Services: Virtual Private Cloud (VPC), Load Balancers & VPNs (Virtual Private Networks) • Database Services: Relational Databases, NoSQL Databases & In-Memory Databases • Security Services: Identity and Access Management (IAM) & Firewalls • Support Services: 24/7 Technical Support, Monitoring & Incident Management 	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.		

Experience	The CSP/MSP should have provisioned cloud services in India for at least Five (05) projects for a value not less than INR 10 Cr each OR at least Three (03) project of value not less than INR 20 Cr in the last 5 years from the last date of bid submission.	Copy of the Purchase order or Letter of Award or Contract of the work. Along with Proof of payments/ Invoices spanning over minimum 12 months. (ANNEXURE-11)		
-------------------	--	--	--	--

7.3. Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted	Provided (Yes/No)	Reference Page No.
Turnover	The CSP shall have an annual turnover of an average INR 500 Cr from cloud business in the last 3 (three) financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24).	Copy of the audited balance sheet for the last three financial years. In case of accounts not finalized yet for the year 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/practising CA, mentioning business from Cloud Services. (ANNEXURE-22)		
Manpower	The bidder should have a minimum 200 certified cloud resources on the proposed cloud platform on their payroll. The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid.	Certified by Company Secretary/ HR along with valid CSP certification along with certificate types. (ANNEXURE-10)		
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: d. ISO/IEC 27018:2019 e. Service and Organization Controls (SOC) 1 f. Service and Organization Controls (SOC) 2	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.		
Managed Databases Features	CSP must have availability of managed databases (PaaS) having features of inbuilt scaling, HA architecture &	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.		

	backup for industry standard databases.			
List of Cloud Services (Tier-I + II)	<p>Services that offer essential and more advanced functionalities compared to the basic services but are not as specialized as the advanced services including but not limited to:</p> <ul style="list-style-type: none"> • Managed Database as a Service: A fully managed cloud database service offering automatic backups, scaling, and high availability without managing infrastructure. • Object Storage: Scalable cloud storage for unstructured data like media files and backups. • File Storage: Cloud storage providing network-attached file systems for shared access across multiple machines. • Native Network Services- VPN Gateway, Public IP & Web Application Firewall (WAF), DN service available in India. • Native Security Services- Cloud Security Posture Management (CSPM), IPDS (Intrusion Prevention and Detection Services) • Monitoring Services- Log Monitoring / Capturing, Operational Metric Collection, Alarm Service & Notification Service • Dedicated CSP Support for Large and Critical Applications: Provides 24/7 expert support for large-scale and mission- 	Undertaking on CSP's letterhead with link to public facing website having the service and functionality description.		

	critical applications in the cloud.			
Experience	The CSP/MSP should have provisioned cloud services in India for at least Four (04) projects for a value not less than INR 40 Cr each OR at least Two (02) project of value not less than INR 80 Cr each in the last 5 years from the last date of bid submission.	Copy of the Purchase order or Letter of Award or Contract of the work. Along with Proof of payments/ Invoices spanning over minimum 12 months. (ANNEXURE-11)		

7.4. Compliance Sheet for CSPs - Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)

Basic Requirement	Eligibility Criteria	Documents to be submitted	Provided (Yes/No)	Reference Page No.
Turnover	The Bidder should have an annual turnover of an average INR 1000 Cr from cloud business in the last 3 financial years ending 31st March 2024 (2021-22, 2022-23, 2023-24)	Copy of the audited balance sheet for the last three years is given. In case of accounts not finalized yet for the year 2023-24, a provisional balance sheet and certificate may be obtained from the statutory auditor/practising CA, mentioning business from Cloud Services. (ANNEXURE-22)		
Manpower	The bidder should have a minimum 300 certified cloud resources on the proposed cloud platform on their payroll. The resources should be on payroll of the bidder for at least 6 months prior to the published date of the bid	Certified by Company Secretary/ HR along with valid CSP certification along with certificate types. (ANNEXURE-10)		
Data Centre Certifications	The CSP should have the following certifications valid as on bid submission date: <ul style="list-style-type: none"> e. ISO/IEC 27018:2019 f. ISO-22301:2019 g. Service and Organization Controls (SOC) 1 	A self-attested copy of certifications awarded to the firm by the concerned accreditation agency/ Organization.		

	h. Service and Organization Controls (SOC) 2			
Managed Databases Features	CSP must have availability of managed databases (PaaS) having features of inbuilt scaling, Multi -AZs HA architecture & backup for industry standard databases.	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.		
List of Cloud Services (Tier-I + II+III)	<p>This category includes specialized and value-added cloud services, including but not limited to:</p> <ul style="list-style-type: none"> • Container Services: Kubernetes-based container orchestration and management. • Managed Database as a Service: Fully managed database services with backup and high availability. • Native Content Delivery Network (CDN): Global content distribution for optimized performance. • Native Security Services: <ul style="list-style-type: none"> • Hardware Security Module (HSM): Dedicated encryption key management services. • DDoS Protection: Enhanced security measures to mitigate cyber threats. • TLS/SSL Certificate Management: Centralized certificate lifecycle management. • Dual/Multi-Factor Authentication: Advanced authentication mechanisms. 	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.		

	<ul style="list-style-type: none"> • Cloud-Native Security Services: SIEM/SOAR, threat protection (cloud workload), etc. • Monitoring Services: Real-time performance and security monitoring. • Native Analytics & AI/ML Services: <ul style="list-style-type: none"> • Analytics Services: AI/ML-enabled analytics, big data processing, and business intelligence. • CSP Managed DevOps Services: Automated DevOps solutions managed by CSPs. • CSP Managed Generative AI Services: AI-driven automation and content generation solutions. 			
Managing of Databases	The bidder should have Managed cloud native enterprise database services for MS-SQL EE, MS-SQL Std., MySQL and PostgreSQL. Similar service experience with value of 50 Cr.	Undertaking by both CSP and MSP on bidder's letterhead with link to public facing website having the service and functionality description.		
Native Advance Services	<ul style="list-style-type: none"> • N/W Security • AIML • LLM • Other advance cloud services. 	Undertaking on bidder's letterhead with link to public facing website having the service and functionality description.		
Experience	The CSP/MSP should have provisioned cloud services in India for at least Four (04) projects for a value not less than INR 200 Cr each OR at least Two (02) project of value not less than INR 400 Cr each in the last 5 years from the last date of bid submission.	Copy of the Purchase order or Letter of Award or Contract of the work. Along with Proof of payments/ Invoices spanning over minimum 12 months. (ANNEXURE-11)		

7.5. Compliance Sheet for MSPs - Pre-Qualification Criteria (applicable for all categories Tier-1, Tier-2 and Tier-3)

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
1	The MSP should be an authorized partner of proposed MeitY empanelled CSPs.	Copy of Authorised partner certificates from CSP, signed by authorized signatory.		
2	The MSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 and in operation for at least 5 years as on 31.03.2025. Consortium or JV not allowed.	Copy of Certificate of Incorporation/Registration/ Partnership deed		
3	The MSP must have a local office in India	Copy of address proof		
4	The MSP must have a positive Net Worth in each of the three FY i.e. FY 21-22, FY 22-23 & FY 23-24 as per last audited financial report.	Certificate from the Statutory Auditor/ Chartered Accountant (ANNEXURE-21)		
5	The MSP should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	Letter signed by the Authorized signatory in the format given in the RFE (ANNEXURE-12)		
6	The MSP should not be subjected to any legal action for any cause in any legal jurisdiction in the last five years.	Undertaking from Authorized signatory on the letter head of the MSP (ANNEXURE-19)		
7	The MSP should provide department the flexibility to create resources like Virtual instance, storage and other services of any configuration and should not restrict to specific configuration.	Letter from Authorized signatory on the letter head of the MSP		
8	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal		

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
9	The platform must offer a fully managed API management solution that enables secure API publishing, supports multi-cloud deployment, and provides advanced scalability features. The solution should be flexible and capable of integrating with a wide range of internal and external API consumers.	URL of the service on the MSP through portal		

7.6. Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-1 for Basic Cloud Services)

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
1	The MSP should have average annual turnover of at least 50 Crore from IT/ITES business in last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant (ANNEXURE-23)		
2	<p>Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central government/PSUs/Public Listed company in India within the last five years as per below:-</p> <ul style="list-style-type: none"> • Five purchase orders each costing not less than the amount equal to Rs 6 Crores OR • Two purchase orders each costing not less than the amount equal to Rs. 15 Crores OR • One purchase orders each costing not less than the amount equal to Rs. 30 Crores 	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)		

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	And bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 6 Crores within the last five years.			
3	<p>The MSP must have strength of at least 30 IT Professionals (Data Centre / networking / system administration / cloud services professional's / cloud security experts etc.) on their payroll.</p> <p>b. The MSP should have minimum 6 certified cloud resources out of the above mentioned 30 resources on their payroll These certified cloud resources should be on Bidder's payroll for 6 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy. (ANNEXURE-10)</p>		
4	<p>The MSP should have at least 3 certification out of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ▪ ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ▪ ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). ▪ ISO 20000-1 (IT service management systems certification, ensuring that the MSP follows best 	Valid Copy of the Certificate to be attached.		

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	<p>practices in IT service management).</p> <ul style="list-style-type: none"> ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 			
5	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal		
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self- provisioning based on the Custom vCPU and RAM - Single Instance SLA: >= 99.5%</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM)</p>	URL of the service on the MSP through portal		
7	The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes	URL of the service through portal		

S.No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	without any reboot of the virtual machine.			
8	The proposed Cloud platform should have security services – The proposed cloud platform should provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, Continuous virtual red teaming including attack paths, risk scoring and toxic combinations.	URL of the service through portal		
9	The platform should offer managed database services for MySQL and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication. The solution must be flexible and compatible with industry standards for database management.	URL of the service through portal		

7.7. Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-2 for Intermediate Cloud Services)

S.No.	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
1	The MSP should have average annual turnover of at least 100 Crore from IT/ITES business in last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant (ANNEXURE-23)		
2	Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central government/PSUs/Public Listed company in India within the last five years as per below:- <ul style="list-style-type: none"> Five purchase orders each costing not less than the amount equal to Rs 8 Crores OR 	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)		

S.No.	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	<ul style="list-style-type: none"> Two purchase orders each costing not less than the amount equal to Rs. 20 Crores OR One purchase orders each costing not less than the amount equal to Rs. 40 Crores <p>And bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 8 Crores within the last five years.</p>			
3	<p>The MSP must have strength of at least 40 IT Professionals (Data Centre / networking / system administration / cloud services professional's / cloud security experts etc.) on their payroll.</p> <p>b. The MSP should have minimum 8 certified cloud resources out of the above mentioned 40 resources on their payroll These certified cloud resources should be on Bidder's payroll for 6 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy. (ANNEXURE-10)</p>		
4	<p>The MSP should have at least 3 certification out of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). ISO 20000-1 (IT service management systems) 	<p>Valid Copy of the Certificate to be attached.</p>		

S.No.	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	<p>certification, ensuring that the MSP follows best practices in IT service management).</p> <ul style="list-style-type: none"> ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 			
5	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal		
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self- provisioning based on the Custom vCPU and RAM - Single Instance SLA: >= 99.5%</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM).</p>	URL of the service on the MSP through portal		
7	The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine.	URL of the service on the MSP through portal		
8	The proposed Cloud should have security services-	URL of the service on the MSP through portal		

S.No.	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	iv. The proposed cloud platform must provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, and a customizable SIEM solution. These security services must be adaptable to multi-cloud environments. v. Continuous virtual red teaming including attack paths, risk scoring and toxic combinations. vi. Cloud security and risk management for multi-cloud environments Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing for multi-cloud.			
9	The platform should offer managed database services for MySQL and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication. The solution must be flexible and compatible with industry standards for database management.	URL of the service on the MSP through portal		

7.8. Compliance Sheet for MSPs - Pre-Qualification Criteria (Tier-3 for Advanced Cloud Services)

S. No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
1	The MSP should have an average annual turnover of at least 200 Crore from IT/ITES business in the last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/ Chartered Accountant (ANNEXURE-23)		
2	Bidder should have successfully implemented / commissioned / maintained project of ICT/ DC-DR/Cloud for any state / central government/PSUs/Public Listed company in India within the last five years as per below:-	Work order + completion Certificate/ CRAC from client (ANNEXURE-11)		

S. No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	<ul style="list-style-type: none"> • Five purchase orders each costing not less than the amount equal to Rs 10 Crores OR • Two purchase orders each costing not less than the amount equal to Rs. 25 Crores OR • One purchase orders each costing not less than the amount equal to Rs. 50 Crores <p>And the bidder should have completed at least one purchase order of IT Security (NGFW/IPS/SIEM/SOAR) costing not less than the amount equal to Rs. 10 Crores within the last five years.</p>			
3	<p>The MSP must have strength of at least 50 IT Professionals (Data Centre / networking / system administration / cloud services professionals / cloud security experts etc.) on their payroll. The MSP should have minimum 30 certified cloud resources of the proposed cloud platform out of the above mentioned on their payroll These certified cloud resources should be on Bidder's payroll for 3 months or more.</p>	<p>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy (ANNEXURE-10)</p>		
4	<p>The MSP must have at least three of the following ISO (International Organization for Standardization) Certifications as on Bid submission Date:</p> <ul style="list-style-type: none"> ▪ ISO 9001 (Quality management systems certification, ensuring consistent quality in products and services.) ▪ ISO 27001 (Information security management systems certification, demonstrating the MSP's commitment to securing sensitive information). 	<p>Valid Copy of the Certificate to be attached.</p>		

S. No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	<ul style="list-style-type: none"> ISO 20000-1 (IT service management systems certification, ensuring that the MSP follows best practices in IT service management). ISO 22301 (Business continuity management systems certification, ensuring the MSP can maintain operations in case of disruptions). ISO 27017 (Cloud security controls certification, addressing cloud-specific information security issues). ISO 27018 (Protection of personal data in the cloud, ensuring the MSP meets privacy protection standards for personal data in cloud environments). 			
5	The MSP must demonstrate their platform's ability to configure and manage high-performance storage, replication, and security services, highlighting its flexibility and scalability for cloud infrastructure, data protection, and security use cases.	URL of the service on the MSP through portal		
6	<p>The MSP should have following services with SLA of:</p> <p>Ease of custom configurations of VM's for self- provisioning based on the Custom vCPU and RAM - Single Instance SLA: >= 99.5%</p> <p>The cloud platform should offer flexible configuration options for compute resources (e.g., vCPU, RAM) and support serverless data lake services with integration capabilities for advanced analytics, including machine learning (ML) and generative AI models. The platform should meet industry-standard SLAs.</p>	URL of the service on the MSP through portal		
7	The proposed Cloud should have Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine.	URL of the service on the MSP through portal		

S. No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
	The cloud platform should support scalable storage with low-latency performance, allow for on-demand scaling without requiring virtual machine reboots, and ensure resilience across multiple availability zones (AZs) or regions. The solution should be flexible and compatible with industry-standard storage protocols.			
8	<p>The proposed Cloud should have security services-</p> <ul style="list-style-type: none"> a. The proposed cloud platform must provide enterprise-grade security services, including but not limited to WAF, DDoS protection, threat detection, vulnerability assessment, and a customizable SIEM solution. These security services must be adaptable to multi-cloud environments. b. Continuous virtual red teaming including attack paths, risk scoring and toxic combinations. c. Cloud security and risk management for multi-cloud environments Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing for multi-cloud. 	URL of the service on the MSP through portal		
9	The cloud platform should support a variety of AI/ML models for tasks such as text generation, summarization, and chatbots, irrespective of whether they are proprietary or open-source. The platform should provide an ecosystem that facilitates seamless integration and deployment of different AI models for various use cases.	URL of the service on the MSP through portal or Demonstrate during the Presentation		
10	The platform should offer CSP Native managed database services for MySQL, MS SQL EE and standard and PostgreSQL that provide high availability, automated backups, scalable storage, and support replication across multiple availability zones or regions. The solution must be flexible and compatible with industry standards for database management.	URL of the service on the MSP through portal		

S. No	Eligibility Criteria	Document to be submitted	Provided (Yes/No)	Reference Page No.
11	<p>The MSP should have Unified End-to-End AI/ML Platform as Managed service that focus on MLOps & LLMOps principles which includes:</p> <ul style="list-style-type: none"> a. The platform should provide a comprehensive, end-to-end AI/ML solution that includes capabilities for model training, versioning, orchestration, and deployment at scale. The platform should also support AI-powered language translation services for a variety of languages, including regional Indian languages, with flexible deployment options. b. Flexible model serving options (online or batch prediction) at scale with optimized infrastructure. c. Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving. d. Platform must provide flexibility to deploy model on a private endpoint and also to be able to export a model to make it portable, like running in a container. e. Language translation service in speech to speech, speech to text, text to speech and text to text for Indian languages. 	URL of the service on the MSP through portal		
12	The platform must offer a fully managed API management solution that enables secure API publishing, supports multi-cloud deployment, and provides advanced scalability features. The solution should be flexible and capable of integrating with a wide range of internal and external API consumers	URL of the service on the MSP through portal		

ANNEXURE 8: Form for Submission of Technical Compliance

8.1. Compliance Sheet for CSPs – Technical Qualification Criteria (Tier-1 for Basic Cloud Services)

S.No	Requirements	Max Marks	Criteria	Marks Obtained
1	All the services should be available from the India Region of the Cloud Service Provider (CSP). CSP should follow the guidelines from MeitY and ensure that all Data and the services used should remain in India.	15	Valid copy of the MeitY certificate	
2	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. The bidder must provide valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.	15	Valid copy of the MeitY certificate Valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.	
3	The Cloud Service Offerings of CSP should be MeitY empanelled & STQC audited as per MeitY empanelment process as on the last date of submission of the bid	15	Valid copy of the MeitY certificate	
4	The CSP must be operating at least two (2) Data Centre / Disaster Recovery Centre Facilities in India located in different seismic zones from the DC, to withstand natural disasters with proven disaster recovery (DR) procedures, including regular testing of failover mechanisms.	25	Valid copy of the MeitY certificate	
5	SLA for its cloud services: - Service Level Agreements (SLA's) for its cloud services - Dashboard with real time service health for all its cloud services across all data centres. Service Level Agreements (SLAs) should guarantee 99.5% uptime and clear timelines for issue resolution. The service health dashboard must be accessible and updated in real-time.	10	CSP Link or Demonstration	

6	<p>Evaluate the ease of provisioning agility, self-service availability of different configurations of VM's for self- provisioning</p> <p>- Service console for provisioning and management of services like server configurations (CPU, memory, storage)</p> <p>- Available offerings/resources: Storage capabilities, Compute capabilities, Database capabilities and types, Networking and Other capabilities</p> <p>Bidders must demonstrate ease of provisioning with self-service availability of VMs, auto-scaling options, and seamless integration with other services.</p>	10	CSP Link or Demonstration	
7	<p>Different types of available storage (e.g. block, object, and file) and data lifecycle process</p> <p>- Establish storage volume and demonstrate/Show how data is loaded and retrieved</p> <p>- Permissions and access management of the volumes</p> <p>The bidder should provide demonstrations of available storage types (block, object, file), with proof of redundancy, failover mechanisms, and access controls for each storage type.</p>	10	CSP Link or Demonstration	

8.2. Compliance Sheet for CSPs – Technical Qualification Criteria (Tier-2 for Intermediate Cloud Services)

S.No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
1	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles.	2	Valid copy of the certificate	

S.No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	The bidder must provide valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.			
2	<p>The CSP should have the following certifications valid as on bid submission date:</p> <p>d. ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards.</p> <p>e. ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.</p> <p>f. ISO/IEC 20000-9 - Guidance on the application of ISO/IEC 20000-1 to cloud services.</p>	5	Valid copy of the certificate	
3	<p>The CSP should provide different options like PAYG, 1-year commit and 3-year commit compute infrastructure and Public pricing/calculator for the price validation and verification. Provide detailed pricing models, including options for PAYG, 1-year, and 3-year commitment plans, with breakdowns of the cost per service</p>	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation	
4	<p>The CSP data lake platform should have End-to-end ML using SQL applications building on the same platform to save the deployment cycle, effort and cost with SLA of 99.95% to enhance the reliability and user experience with capabilities of GenAI Integration and inbuilt Machine learning models.</p>	5	URL of the service on the CSP Product Page	
5	<p>The CSP should have managed security services-</p> <p>f. WAF & DDoS Protection with enterprise features such as Threat Intelligence, Third-party named IP address & Adaptive Protection</p> <p>g. Threat detection, Vulnerability Assessment, Bot management with captcha Integration</p> <p>h. Cloud Native Security services – IPDS</p> <p>i. Continuous virtual red teaming including attack paths, risk</p>	5	URL of the service on the CSP Product Page	

S.No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	scoring, and toxic combinations, j. Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing			
6	The CSP should have State-of-the-art multi-modal LLMs for Text Generation, Summarization, Chatbots and Conversational with deployable options on the CSP managed AI/ML Platform.	7	Public Links and Letter from Authorized signatory on the letter head of the bidder.	
7	The CSP should have Managed cloud native enterprise database services for MySQL and PostgreSQL with the following features: a. Enterprise Database services with 99.5% SLA b. Automated backups and point-in-time recovery or equivalent c. Automatic Storage Increase d. Automated replication / Automatic failover to another Zone e. HA architecture with Sync/async replication.	10	Public Links and Letter from Authorized signatory on the letter head of the bidder.	
8	The CSP should have Managed cloud Kubernetes service with the following features: d. Secure Verified Container Images for software supply-chain security e. Container Threat Detection as inbuilt service with Dashboard f. Vertical/Horizontal Pod Autoscaler and Node auto-upgrades	5	Public Links and Letter from Authorized signatory on the letter head of the bidder.	
9	The CSP must have GPU based machines with unified End-to-End AI/ML Platform as Managed service as one of the publicly listed services. The minimum Technical Specifications of GPUs: c. FP32 - 30.3 tera FLOPs or above configuration d. GPU Memory- 24 GB or above configuration	2	Public Links and Letter from Authorized signatory on the letter head of the bidder.	
10	The CSP should have centralized security solution providing a single, consolidated view of the organization	2	URL of the service on the CSP through Self provisioning portal	

S.No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	security posture covering the following features: <ul style="list-style-type: none"> • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring • Risk Prioritization • Incident Response • Discovery and Inventory 			
11	The CSP should have the CDN service.	5	URL of the service on the CSP Product Page/Marketplace	
12	The CSP should have Managed cloud Auto-Scaling capabilities with the following features: <ul style="list-style-type: none"> - Predictive autoscaling by forecasting future load & scaling out in advance or equivalent - Schedule-based autoscaling - Utilization metrics based autoscaling The bidder should demonstrate their auto-scaling capabilities, including predictive scaling based on load forecasts, and provide case studies or performance metrics to validate the effectiveness or the bidder needs to set threshold for CPU and RAM, to achieve autoscaling with desired performance.	2	URL of the service on the CSP Product Page	
13	The CSP Should have Managed Object storage service with the following features: <ul style="list-style-type: none"> - Object's lifecycle by using a lifecycle configuration - Support read-after-write consistency for addition of any object - No minimum billable object size - Data Exfiltration control - Default data encryption at rest - Ability to charge requester for data retrieval cost 	7	URL of the service on the CSP Product Page	
14	The CSP should have Managed cloud NoSQL database services with the following features <ul style="list-style-type: none"> -Serverless NoSQL key value pair document DB -Automated replication to different zones/geo-resilient data centres. -Encryption at rest 	2	URL of the service on the CSP Product Page	

S.No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	-Fully managed with no planned downtime			
15	The CSP should support the Managed Hadoop Service	2	URL of the service on the CSP Product Page	
16	<p>The CSP should have Managed Security Services with following features:</p> <ul style="list-style-type: none"> -Web Application Firewall supporting TOP 10 OWASP -DDoS Protection -Threat detection, Vulnerability Assessment, -Identity and Access Management - fine grained access control for access to cloud resources -Single Sign-On & Multi factor Authentication - Cloud HSM & Key Mgmt. - Password Management -SSL Certificate -Discover, classify, and protect data using native Data Loss Prevention -Real-time log management and analysis -Identity and context to guard the access of VMs and Applications 	7	URL of the service on the CSP Product Page	
17	<p>The CSP should have Managed Backup & DR Service with following features:</p> <ul style="list-style-type: none"> -Instant mount and recovery -Application-consistent backups -Application-aware backup and recovery for databases 	5	URL of the service on the CSP Product Page	
18	<p>The CSP should have the following managed networking services:</p> <ul style="list-style-type: none"> - IPv4, IPv6 - DHCP - IPSec VPN Tunnel Creation - Geo/Network load Balance (Balancing between multiple sites) - Load Balancer. (Internal and External Load Balancers) - L3 and L4 Anti-DDoS solution 	2	URL of the service on the CSP Product Page	
19	Details Demo and Presentation of Database as service Active/Standby and DR automatic replication, Kubernetes as services with sample application monitoring & Pods Scaling, Backup and DR configuration for MS-SQL Database running on VMs, GPUs Machines with flexibility to add/remove GPUs on demand etc.	20	In-Person Demonstration of the required services	

8.3. Compliance Sheet for CSPs - Technical Qualification Criteria (Tier-3 for Advanced Cloud Services)

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
1	<p>The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles.</p> <p>The bidder must provide valid, up-to-date copies of SOC 1, SOC 2, certificates for the last audit cycle.</p>	2	Valid copy of the certificate	
2	<p>The CSP should have the following certifications valid as on bid submission date:</p> <ul style="list-style-type: none"> g. ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards. h. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology. i. ISO 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds. j. ISO-22301 for Business Continuity Management. k. ISO/IEC 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services. l. ISO/IEC 42001:2023 - Information technology — Artificial intelligence — Management system 	5	Valid copy of the certificate	
3	CSP should provide different options like PAYG, 1 year commit and 3 year commit compute infrastructure with different list pricing per selection e.g. On-Demand, 1, 3 years etc. and Public pricing/calculator for the price validation and verification.	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation	
4	The CSP data lake platform should have End-to-end ML using SQL applications building on the same platform to save the deployment cycle, effort and cost with SLA of 99.95% to enhance the reliability and user experience with capabilities of GenAI	5	URL of the service on the CSP Product Page	

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	Integration and inbuilt Machine learning models.			
5	<p>The CSP should have Native security services-</p> <ol style="list-style-type: none"> WAF & DDoS Protection with enterprise features such as Threat Intelligence, Third-party named IP address & Adaptive Protection Threat detection, Vulnerability Assessment, Bot management with captcha Integration Cloud Native Security services – IPDS Continuous virtual red teaming including attack paths, risk scoring, and toxic combinations Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing 	5	URL of the service on the CSP Product Page	
6	CSP should have native State-of-the-art multi-modal LLMs for Text Generation, Summarization, Chatbots and Conversational with deployable options on the CSP native fully managed AI/ML Platform.	5	URL of the service on the CSP Product Page or Demonstrate during the Presentation	
7	<p>The CSP should have Managed cloud native enterprise database services for MS-SQL EE, MS-SQL Std., MySQL and PostgreSQL with the following features:</p> <ol style="list-style-type: none"> Enterprise Database services with synchronous replication and automatic failover of a primary database to a standby database copy in a separate physical data centre in the same region to ensure high availability and low latency. Automated backups and point-in-time recovery for database lifecycle management e.g. Provisioning, de-provisioning, patching, backups, DR configuration, HA etc. Automatic Storage Increase Redundant Zone High Availability (HA) architecture with automated 	10	URL of the service on the CSP Product Page	

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	<p>replication and automatic failover to another availability zone.</p> <p>e. Redundant Zone HA architecture with self-service public APIs for managing database functions, including start/stop, backup, restoration, configuration, and scaling.</p>			
8	<p>The CSP should have native Unified End-to-End AI/ML Platform as Managed service that focus on MLOps & LLMOps principles which includes:</p> <ul style="list-style-type: none"> a. Managed services for Model training b. Build, orchestrate, and automate reproducible ML workflows, easing the transition from experimentation to production c. Centralized repository for managing, versioning, and tracking trained ML models d. Flexible model serving options (online or batch prediction) at scale with optimized infrastructure e. Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving f. Platform must provide flexibility to deploy model on a private endpoint and also to be able to export a model to make it portable, like running in a container" g. Language translation service in speech to speech, speech to text, text to speech and text to text for Indian languages. 	7	URL of the service on the CSP Product Page	
9	<p>CSP must offer Kubernetes/Containerized environment that should have following capabilities from Day 1:</p> <ul style="list-style-type: none"> a. Capability for regional clusters to replicate cluster masters and nodes across multiple zones within a single region. b. Kubernetes resources are spread across multiple zones of a region c. K8S cluster must provide features to help keep the platform secure with automatic upgrades of the node OS and Kubernetes components via Automatic Node Upgrades. 	5	URL of the service on the CSP Product Page	

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	<p>d. CSP should provide tools for application modernization like Native managed Kubernetes services and CSP Native CI/CD pipelines.</p> <p>e. Secure Verified Container Images for software supply-chain security</p>			
10	<p>The CSP must have GPU based machines with unified native End-to-End AI/ML Platform as Managed service as one of the publicly listed services. The minimum Technical Specifications of GPUs:</p> <p>a. FP32 - 30.3 teraflops Or Above Configuration</p> <p>b. GPU Memory- 24 GB/GPU or Above Configuration</p>	2	Public Links and Letter from Authorized signatory on the letter head of the bidder.	
11	<p>Centralized Security solution providing a single, consolidated view of the organization security posture covering the following features:</p> <ul style="list-style-type: none"> • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring • Risk Prioritization • Incident Response • Discovery and Inventory 	2	URL of the service on the CSP Product Page	
12	The CSP should have Native CDN service with Compliances.	10	CSP Native Public Links and Letter from Authorized signatory on the letter head of the bidder.	
13	<p>The CSP should have Managed Compute Services with the following features:</p> <ul style="list-style-type: none"> - Container Optimize O/S - Option to disable Simultaneous Multi-Threading (SMT) - Scheduler for Start and Pause to preserves the state of a VM on restart -CSP Native Linux Images like - RHEL, SUSE, Debian, Ubuntu with native billing for RHEL & SUSE. 	6	URL of the service on the CSP Product Page	
14	<p>The CSP should have Managed cloud native Auto-Scaling capabilities with the following features:</p> <ul style="list-style-type: none"> - Predictive autoscaling by forecasting future load & scaling out in advance - Schedule-based autoscaling - Utilization metrics based autoscaling 	2	URL of the service on the CSP Product Page	

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
15	The CSP should have the Managed cloud native Serverless computing	2	URL of the service on the CSP Product Page	
16	The CSP should have Managed Object storage service with the following features: <ul style="list-style-type: none"> - Average sub millisecond retrieval time including archival tier - Object's lifecycle by using a lifecycle configuration - Support read-after-write consistency for addition of any object - No minimum billable object size - Data Exfiltration control - Default data encryption at rest - Ability to charge requester for data retrieval cost 	3	URL of the service on the CSP Product Page	
17	The CSP should have Managed cloud native NoSQL database services with the following features <ul style="list-style-type: none"> -Serverless NoSQL key value pair document DB -Automated replication to different zones -Encryption at rest -Fully managed with no planned downtime 	1	URL of the service on the CSP Product Page	
18	The CSP should support the Managed Hadoop Service	1	URL of the service on the CSP Product Page	
19	The CSP should have Managed Security Services with following features: <ul style="list-style-type: none"> -Web Application Firewall supporting TOP 10 OWASP -DDoS Protection -Threat detection, Vulnerability Assessment, -Identity and Access Management - fine grained access control for access to cloud resources -Single Sign-On & Multi factor Authentication - Cloud HSM & Key Mgmt. - Password Management -SSL Certificate -Discover, classify, and protect data using native Data Loss Prevention -Real-time log management and analysis -Identity and context to guard the access of VMs and Applications 	2	URL of the service on the CSP Product Page	
20	The CSP should have Managed native Backup & DR Service with following features:	4	URL of the service on the	

S. No	Evaluation Criteria	Max Marks	Criteria	Marks Obtained
	-Instant mount and recovery -Application-consistent backups -Application-aware backup and recovery for databases		CSP Product Page	
21	The CSP should have the following managed networking services: - IPv4, IPv6 - DHCP - IPsec VPN Tunnel Creation - Geo load Balance (Balancing between multiple sites) - Load Balancer. (Internal and External Load Balancers) - L3 and L4 Anti-DDoS solution	1	URL of the service on the CSP Product Page	
22	Details Demo and Presentation of CSP Native Auto-scaling, Compute Services with O/S Images of RHEL, SUSE native billing, Multi-Threading (SMT) of vCPUs, Consolidated view of the security posture, Native CDN integration with Cloud Services & Unified AI Platform with GPUs training options, CSP native MS-SQL EE. Database as service Active/Standby and DR automatic/inbuilt replication to different Regions/DCs.	15	In-Person Demonstration of the required services	

ANNEXURE 9: Indicative Bill of Quantities (BoQ)

The bidder is required to fill the Unit Price (D) in the table below. Based on the service category weight and indicative BoQ; the total price against each service will be calculated.

9.1. BoQ for Tier-1 (Basic Cloud Services)

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
A. Compute as Managed Service										
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730				
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
13			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
14			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
17			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
18			VM - 2 vCPU, 16GB RAM	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
19			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
20			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
21			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
22			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
23			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
24			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
25			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
26			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
28			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
29			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
30		Windows Standard edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730				
31			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
32			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
33			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
34			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
35			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
36			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
37			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
39			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
40		Windows Datacenter edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730				
41			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
42			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
43			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
44			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
45			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
46			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
47			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
48			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
B. Storage as a Managed Service - Object, File and Block Storage										
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly				
2	Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly				
3	Managed Storage- SSD	Managed SSD Storage for Mission Critical Web, Apps & DB	Single SSD redundant volume from Storage tier which support single-digit millisecond latency without Disk Striping	1 GB Per Month	5	Monthly				
				10 GB Per Month	5	Monthly				
				100 GB Per Month	5	Monthly				
				500 GB Per Month	5	Monthly				
				1000 GB Per Month	5	Monthly				
				2000 GB Per Month	5	Monthly				
				3000 GB Per Month	5	Monthly				
				4000 GB Per Month	5	Monthly				
				5000 GB Per Month	5	Monthly				
				10000 GB Per Month	5	Monthly				
C. CSP/MSP Managed DB - Managed services										
1	Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL/My-SQL as a service with automated backups and point- in-time recovery	2 vCPU 8 GB RAM	Hourly	2	730				
2			4 vCPU 16 GB RAM	Hourly	2	730				
3			8 vCPU 32 GB RAM	Hourly	2	730				
4			16 vCPU 64 GB RAM	Hourly	2	730				
5			32 vCPU 128 GB RAM	Hourly	2	730				
6			48 vCPU 192 GB RAM	Hourly	2	730				
7			64 vCPU 256 GB RAM	Hourly	2	730				
8			96 vCPU 384 GB RAM	Hourly	2	730				
D. Other Managed / Additional Services / Network /Back-up / Security										

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
1	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly				
2	Site to Site VPN - Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly				
3	Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
4	Managed TCP Load balancer(L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
5	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly				
6	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	1	Monthly				
7	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly				
8	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
9	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly				
10	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly				
11	Managed DDoS Protection and WAF	Web Application Firewall as Managed service	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly				
12	Network Firewall - NGFW	Managed Network Firewall - IPDS NGFW	Managed Network Firewall with intrusion detection / prevention system with 4 Gbps throughput	Monthly	1	Monthly				

9.2. BoQ for Tier-2 (Intermediate Cloud Services)

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
A. Compute as Managed Service										
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730				
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
13			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
14			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
17			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
18			VM - 2 vCPU, 16GB RAM	Hourly	1	730				
19			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
20			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
21			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
22			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
23			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
24			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
25			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
26			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
28			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
29			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
30		Windows Standard edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730				
31			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
32			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
33			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
34			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
35			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
36			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
37			VM - 80 vCPU, 320 GB RAM	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL	
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]	
38			VM - 96 vCPU, 384 GB RAM	Hourly	1	730					
39			Windows Datacenter edition O/S with O/S Licenses	VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
40				VM - 2 vCPU, 8GB RAM	Hourly	1	730				
41		VM - 4 vCPU, 16GB RAM		Hourly	1	730					
42		VM - 8 vCPU, 32GB RAM		Hourly	1	730					
43		VM - 16 vCPU, 64GB RAM		Hourly	1	730					
44		VM - 32 vCPU, 128GB RAM		Hourly	1	730					
45		VM - 48 vCPU, 192GB RAM		Hourly	1	730					
46		VM - 64 vCPU, 256 GB RAM		Hourly	1	730					
47		VM - 80 vCPU, 320 GB RAM		Hourly	1	730					
48		VM - 96 vCPU, 384 GB RAM		Hourly	1	730					
49		VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
B. Storage as a Managed Service - Object, File and Block Storage											
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly					
2	Archive Storage	Managed Archival Storage	Fully Managed Geo Redundant Archival/ Cold Tier	TB per month	100	Monthly					
3	Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly					
4	Managed Storage-SSD	Managed SSD Storage for Mission Critical Web, Apps & DB	Single SSD redundant volume from Storage tier which support single-digit millisecond latency without Disk Striping	1 GB Per Month	5	Monthly					
				10 GB Per Month	5	Monthly					
				100 GB Per Month	5	Monthly					
				500 GB Per Month	5	Monthly					
				1000 GB Per Month	5	Monthly					
				2000 GB Per Month	5	Monthly					
				3000 GB Per Month	5	Monthly					
				4000 GB Per Month	5	Monthly					

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
				5000 GB Per Month	5	Monthly				
				10000 GB Per Month	5	Monthly				
C. CSP/MSP Managed DB - Managed services										
1	Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL/My-SQL as a service with following features: a) Automated backups and point-in-time recovery or equivalent b) Automatic Storage Increase c) Should support horizontal scaling by adding/removing read replicas. Bidder must quote the Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	2 vCPU 8 GB RAM	Hourly	2	730				
2			4 vCPU 16 GB RAM	Hourly	2	730				
3			8 vCPU 32 GB RAM	Hourly	2	730				
4			16 vCPU 64 GB RAM	Hourly	2	730				
5			32 vCPU 128 GB RAM	Hourly	2	730				
6			48 vCPU 96 GB RAM	Hourly	2	730				
7			64 vCPU 128 GB RAM	Hourly	2	730				
8			96 vCPU 256 GB RAM	Hourly	2	730				
D. Other Managed / Additional Services / Network / Back-up / Security										
1	Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100GB/Month	1	Monthly				
2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support service mesh for observability, network and security.	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly				
4	Site to Site VPN - Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly				
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	1	Monthly				
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100hrs/Per month	1	Monthly				
7	Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
8	Managed TCP Load balancer(L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly				
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	1	Monthly				
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features:	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
		- Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy								
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly				
13	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly				
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly				
16	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and get visibility of cloud assets and resources on single Dashboard	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed/month	10	Event/cloud operation per month				
17	Managed DdoS Protection and WAF	Web Application Firewall as Managed service	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly				
18	Network Firewall - NGFW	Managed Network Firewall - IPDS NGFW	Managed Network Firewall with intrusion detection / prevention system with 4 Gbps throughput	Monthly	1	Monthly				
E. Content Delivery Network (CDN)										
1	Managed Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	1	Monthly				
F. GPU As Service										
1	Production Grade Virtual Machine with GPU	GPU Config: FP32 - 30.3 teraFLOPs Or Above Configuration and GPU Memory- 24 GB/GPU or Above Configuration) with	VM - 2 vCPU, 16GB RAM, 1 GPU	Hourly	1	730				
2			VM - 8 vCPU, 32GB RAM, 1 GPU	Hourly	1	730				
3			VM - 12 vCPU, 48GB RAM, 1 GPU	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
4		Virtual Machine Configuration	VM - 16 vCPU, 64GB RAM, 1 GPU	Hourly	1	730				
5			VM - 32 vCPU, 128GB RAM, 1 GPU	Hourly	1	730				
6			VM - 24 vCPU, 96GB RAM, 2 GPU	Hourly	1	730				
7			VM - 48 vCPU, 192GB RAM, 4 GPU	Hourly	1	730				
8			VM - 96 vCPU, 384 GB RAM, 8 GPU	Hourly	1	730				

9.3. BoQ for Tier-3 (Advanced Cloud Services)

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
A. Compute as Managed Service										
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730				
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
12			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
13			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
14		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730				
15			VM - 2 vCPU, 8GB RAM	Hourly	1	730				
16			VM - 2 vCPU, 16GB RAM	Hourly	1	730				
17			VM - 4 vCPU, 8GB RAM	Hourly	1	730				
18			VM - 4 vCPU, 16GB RAM	Hourly	1	730				
19			VM - 4 vCPU, 32GB RAM	Hourly	1	730				
20			VM - 8 vCPU, 32GB RAM	Hourly	1	730				
21			VM - 16 vCPU, 64GB RAM	Hourly	1	730				
22			VM - 32 vCPU, 128GB RAM	Hourly	1	730				
23			VM - 48 vCPU, 192GB RAM	Hourly	1	730				
24			VM - 64 vCPU, 256 GB RAM	Hourly	1	730				
25			VM - 96 vCPU, 384 GB RAM	Hourly	1	730				
26			VM - 128 vCPU, 512 GB RAM	Hourly	1	730				
27		Windows Standard edition O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Hourly	1	100				
28			VM - 4 vCPU, 16GB RAM	Hourly	1	100				
29		** O/S Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding)	VM - 8 vCPU, 32GB RAM	Hourly	1	100				
30			VM - 16 vCPU, 64GB RAM	Hourly	1	100				
31			VM - 32 vCPU, 128GB RAM	Hourly	1	100				
32		Windows Datacenter edition O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Hourly	1	100				
33			VM - 4 vCPU, 16GB RAM	Hourly	1	100				
34			VM - 8 vCPU, 32GB RAM	Hourly	1	100				
35			VM - 16 vCPU, 64GB RAM	Hourly	1	100				
36		** O/S Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding)	VM - 32 vCPU, 128GB RAM	Hourly	1	100				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
37	Function as a Service	Bidder must quote Serverless, event-driven compute service that let developers run code without provisioning or managing servers	1 GB RAM , Requests per month (millions) =1 and Average execution time per request (ms)= 1000 ms	Hourly	1	730				
38	Serverless Compute as a Service	Fully managed Serverless compute for containers: a) Linux Support b) OS updates c) underlying infrastructure d) dynamically scale capacity in response to changes in demand to reduce waste e) highly available	Serverless compute with 1 vCPU 4 GB RAM	Hourly	1	730				
39			Serverless compute with 2 vCPU 8 GB RAM	Hourly	1	730				
B. Storage as a Managed Service - Object, File and Block Storage										
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly				
2	Archive Storage with milliseconds restore tier	Managed Archival Storage - Restored quickly in milliseconds	Fully Managed Geo Redundant Archival/ Cold Tier with instant restore time	TB per month	100	Monthly				
3	Cloud Native Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly				
4	Managed Storage-SSD	Managed SSD Storage for Mission Critical Web, Apps & Databases	Single SSD redundant volume from Storage tier which support Sub-millisecond latency performance.	1 GB Per Month	5	Monthly				
				10 GB Per Month	5	Monthly				
				100 GB Per Month	5	Monthly				
				500 GB Per Month	5	Monthly				
				1000 GB Per Month	5	Monthly				
				2000 GB Per Month	5	Monthly				
				3000 GB Per Month	5	Monthly				
				4000 GB Per Month	5	Monthly				
				5000 GB Per Month	5	Monthly				
				10000 GB Per Month	5	Monthly				
C. Managed DB - Native Managed services by CSP										
1			2 vCPU 8 GB RAM	Hourly	2	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
2	CSP Native Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	4 vCPU 16 GB RAM	Hourly	2	730				
3			8 vCPU 32 GB RAM	Hourly	2	730				
4			16 vCPU 64 GB RAM	Hourly	2	730				
5			32 vCPU 128 GB RAM	Hourly	2	730				
6			48 vCPU 96 GB RAM	Hourly	2	730				
7			64 vCPU 128 GB RAM	Hourly	2	730				
8			96 vCPU 256 GB RAM	Hourly	2	730				
9		MS SQL Server 2017 / 2019 / 2022 Enterprise/Standard as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) MS-SQL Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding) Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	2 vCPU 4 GB RAM	Hourly	1	100				
10			4 vCPU 8 GB RAM	Hourly	1	100				
11			8 vCPU 16 GB RAM	Hourly	1	100				
12			16 vCPU 32 GB RAM	Hourly	1	100				
13			130 GB Enterprise Grade Redis with Sharding support	Monthly	2	Monthly				
	CSP Native Redis Cluster as Service - Production Grade supporting Sharding	Managed Redis as a Service with: - Should support the Managed Cache database service - Supports partitions/shards and read replicas - Must be compatible with open-source Redis data store - Inbuilt capability to auto-scale								

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
		shards and read replicas - Shards data across Redis nodes								
14	Production Grade CSP Native Managed Non-Relational Database(NoSQL) as Managed Services	Scalable NoSQL DB as Managed Service 1) Automated replication/Automatic failover to another Zone and region 2)Automated Backup 3)Multi -AZs HA architecture	Storage (GB) - 50 , Number of writes / Second: 1000 , Number of reads / Second: 2000, Backup - 30 days	Monthly	2	Monthly				
D. Other CSP Managed / Additional Services / Network / Back-up / Security										
1	CSP native Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100GB/Month	1	Monthly				
2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support service mesh for observability, network and security.	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	1	730				
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly				
4	Site to Site VPN - CSP Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly				
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	1	Monthly				
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100hrs/Per month	1	Monthly				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
7	CSP Natively Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
8	CSP Natively Managed TCP Load balancer(L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly				
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly				
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	1	Monthly				
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly				
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly				
13	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly				
14	Messaging services	Should provide a managed message queueing service for communicating between decoupled application components	Standard queue requests and FIFO queue requests in millions /1GB Volume with number of Subscriptions per Month	Monthly	1	Monthly				
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]		[10]	[11]
16	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and get visibility of cloud assets and resources on single Dashboard	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed/month	10	Event/cloud operation per month				
17	Managed DDoS Protection and WAF	Web Application Firewall CSP Natively Managed	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly				
18	Network Firewall - Cloud Native NGFW	CSP Native Managed Network Firewall - IPDS NGFW with Transport Layer Security (TLS) interception and decryption	Managed Network Firewall with intrusion detection / prevention system. Each firewall endpoint will process 50 Terabyte of traffic /50 TB data processed per month , the Billing will be based on the actual consumption	Monthly	1	Monthly				
E. CSP Native Content Delivery Network (CDN)										
1	Managed CSP Native Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	1	Monthly				
F. CSP Native AI/ML & Data Warehouse Platform										
1	ML Notebook	Fully managed CSP native Notebook IDE - Fully Managed & collaborative Jupyter Notebook - to perform all ML development steps (Prepare, build, Train & Deploy) from a single Web based visual interface.	Node Size 16 vCPU 64 GB RAM	Monthly	2	730				
2	ML Training	Fully managed CSP native Training Jobs Service: GPU-powered instances for running training jobs. One Node - (24vCPU, 96GB of memory, 2 Nos of GPUs that supports TensorFlow, PyTorch, XgBoost ML-API for training Models and network performance of 32 Gbps)	Node Size: 24vCPU, 96 GB RAM with 2 GPUs / training job per month/730hrs	Monthly	2	730				
3	ML Inference	Real Time Inference	Node Size 16 vCPU 64 GB RAM	Monthly	2	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR) [9] = [6]x [7]x [8]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
4	Fully Managed Data Warehouse	Full managed Datawarehouse with - Cloud-based enterprise data warehouse (EDW) to run complex queries across petabytes of data.	Data Warehouse Platform: a. Cloud-based enterprise Data warehouse - each unit/node having minimum configuration of 4 vCPU & 32 GB RAM, for running complex Queries(Approximate 100 Queries in Month with each query scanning of minimum of 100GB of data with 4 dedicated nodes/units (1 leader node & 3 workers) for Number of units in estimated units with 100% utilization of dedicated nodes; Or b. Fully Managed Cloud-based Serverless data warehouse - should run complex queries (Approximate 100 Queries in Month with each query scanning minimum of 100GB of data for Number of units in estimated units) Pls Note: Bidder to quote only one (either a or b) option, which must support HA cluster deployment & Data Governance features including Row level Security , Data Masking, and cluster encryption using Customer Managed Key	Monthly	1	730				
5	Managed ETL as a Service	Managed ETL Service: - Serverless service to process and transfer data between different compute and storage services data sources at specified intervals, create, schedule, orchestrate and manage data pipelines	4vCPU and 16GB	Monthly	1	730				
6	Data Visualization /BI Service	Fully Managed Serverless service with - Auto-scalable - Data visualization service for	Data Visualization Service	Monthly	1	730				

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Total Monthly Cost (CSP public pricing in INR)	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9] = [6]x [7]x [8]	[10]	[11]
		telemetry data and operational metrics								
G. Generative AI As Service										
1	GenAI - Multimodal models/LLM Model hosted in India (As a service/hosted on CSP native AI Managed service)	Multimodal Managed large model API for Image, Video, Text & Audio	Image Input/image	million/Month	1	Monthly				
2			Video Input/second	1000000	1	Monthly				
3			Text Input & output – Token equivalent	million/Month	1	Monthly				
4			Audio Input/second	1000000	1	Monthly				
H. GPU As Service										
1	Production Grade Virtual Machine with GPU	GPU Config: FP32 - 30 teraFLOPs Or Above Configuration and GPU Memory- 24 GB/GPU or Above Configuration) with Virtual Machine Configuration : Similar or higher as per Shape available on the CSP console	VM - 2 vCPU, 16GB RAM, 1 GPU	Hourly	1	730				
2			VM - 8 vCPU, 32GB RAM, 1 GPU	Hourly	1	730				
3			VM - 12 vCPU, 48GB RAM, 1 GPU	Hourly	1	730				
4			VM - 16 vCPU, 64GB RAM, 1 GPU	Hourly	1	730				
5			VM - 32 vCPU, 128GB RAM, 1 GPU	Hourly	1	730				
6			VM - 24 vCPU, 96GB RAM, 2 GPU	Hourly	1	730				
7			VM - 48 vCPU, 192GB RAM, 4 GPU	Hourly	1	730				
8			VM - 96 vCPU, 384 GB RAM, 8 GPU	Hourly	1	730				
9		GPU Config: FP32 - 60 teraFLOPS FP16 - 1600 teraFLOPS GPU Memory- 141 GB/GPU or Above Configuration with Multi-Instance GPUs MIGs support	VM - 192 vCPU, 2048 GB RAM with 8 GPUs	Hourly	1	100				

ANNEXURE 10: Undertaking from HR demonstrating its Organization Strength

<On Company's Letter Head>

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Sub: Undertaking for employees on company pay-roll as on Bid Publishing date

Ref: Bid No: <RFE Reference Number here>Dated <DD/MM/YYYY>

Dear Sir,

This is also to certify that <Mention Bidder's company Name> have below mentioned number of employees on company's payroll as on Bid Submission date.

At least <Mention the total number of professionals> of these professionals have experience (of minimum 5 years) in maintenance of cloud solution/ DR Management / virtual server administration/system administration, Virtualization, security, database etc.

S. No.	Resource Profile	Number of Employees on Company's Payroll as on Bid submission date
1.	Data Centre professionals	
2.	Networking professionals	
3.	System Administration professionals	
4.	Cloud Services professionals	
5.	Cloud Security professionals	

Yours Sincerely,

On behalf of [Bidder's Name]

Authorized Signature [In full and initials]:

Name & Title of Signatory:

Name of Firm:

Address:

Seal/Stamp of the Bidder:

ANNEXURE 11: Format for Project Experience

<Attach separate table for each project>

The bidder shall submit its experience with respect to Projects executed, reckoned from the last date of original bid submission. The details regarding the projects executed shall be tabulated as per table below:

S. No.	Details of the Project	Description
1.	Project Title	
2.	Name of the Client & Address	
3.	Client Contact (Name, Designation, Email ID)	
4.	Project Start Date	
5.	Project End Date	
6.	Total Project Value	
7.	Year wise billing	
8.	Narrative description of the project (not more than 500 words)	
9.	Description of services provided within the project (not more than 500 words)	

The bidder agrees that the purchaser may contact the respective clients to verify the details provided. Only the projects listed in the above table will be considered by the purchaser. Any project mentioned without supporting documents will not be considered for evaluation.

The purchaser reserves the right to seek clarification regarding the projects executed by the bidder.

The bidder acknowledges and understands that providing false or misleading information may result in disqualification of the bid.

Declaration

I, the undersigned, certify to the best of my knowledge and belief, that the information contained in this form correctly describes my experience.

Signature of authorized representative of the Bidder:

Date:

Signature

Place:

Full Name of Authorized Signatory

Designation.....

Contact Details & Address.....

ANNEXURE 12: Self-declaration for Non-Blacklisting

(Self-certification in Company's letterhead)

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 NICSI or any of the Central or State Government Organisation / Public Sector Undertaking / Autonomous Body etc.

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 NICSI, or any other Central or State Government Organisation / 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/RFEs.

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

(Signature of Bidder with Seal)

Name:

Capacity in which as signed:

Name & address of the Company / Firm:

Date:

Place:

ANNEXURE 13: Undertaking on Absence of Conflict of Interest

<Original signed copy on company letterhead>

[Date]

Undertaking on Absence of Conflict of Interest

I/We as Applicant do hereby undertake that there is absence of actual or potential conflict of interest on the part of our organization or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with NICSI. I/We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of our organization to comply with the requirements as given in the application document.

We undertake and agree to indemnify and hold NICSI harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) by NICSI and/or its representatives, if any such conflict arises later.

Yours faithfully,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 14: Commercial Cover Letter

<On Company's Letter Head>

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Sub: Submission of Commercial Bid for RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services

Ref: Bid No: <RFE Reference Number here>Dated <DD/MM/YYYY>

Dear Sir,

We, [Bidder's Company Name], are pleased to submit our **Commercial Bid** in response to the **[RFE No.]** dated **[RFE Date]** for **[RFE Name]**. We have carefully reviewed the requirements specified in the RFE and hereby offer our pricing proposal in accordance with the terms and conditions outlined.

1. Price and Validity

All the prices mentioned in our bid are in accordance with the terms as specified in the bid documents. All the prices and other terms and conditions of this bid are valid for a period of 180 calendar days from the date of opening of the Bids.

We hereby confirm that our bid prices include all taxes. We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other Corporate Tax in altered under the law, we shall pay the same.

2. Unit Rates

We have indicated in the relevant schedules enclosed, the unit rates for the purpose of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. Deviations

We declare that all the services shall be performed strictly in accordance with the bid documents and there are no deviations.

4. Qualifying Data

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

5. Bid Price

We declare that our Bid Price is for the entire scope of the work as specified in the bid document. These prices are indicated in the subsequent sub-sections of this Section.

6. Security Deposit

We hereby declare that in case the contract is awarded to us, we shall submit the Security Deposit.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a bid you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 15: Abridged Financial Bid

Name of the Bidder: _____

Tier Category: _____ (Mention the Tier for which the bid has been submitted)

15.1 GROSS TOTAL VALUE (GTV)

GROSS TOTAL VALUE (X)	Rs. (in figures)
	Rs. (in words)

Note:

- Prices should be quoted in Indian Rupee only and indicated both in figures and words. The amount mentioned in words will prevail.
- The bidder at first should calculate the value of GTV(X) in detailed financial bid.
- The Gross Total Value (GTV) shall be inclusive of the total cost of all quoted services for applicable service categories under respective tiers (Tier-1: Annexure-16.1 / Tier-2: Annexure-16.2 / Tier-3: Annexure-16.3) and the total cost of all quoted manpower/resources (Annexure-16.4). For example, in Tier-1 the GTV will be sum of column [11] of table 16.1 + Grand Total (A+B+C) of table 16.4.
- In this proforma, the GROSS TOTAL VALUE (X) as calculated in Detailed Financial Bid has to be reproduced as above.
- This proforma shouldn't contain any detailed rates otherwise the bid will be rejected.

ANNEXURE 16: Detailed Financial Bid

Ref.: <RFE Reference Number here> dated <DD/MM/YYYY>

Name of the Bidder:

The offer with rates for the schedule of requirements of items, as elaborated under, is to be submitted. Adhering to the format given below is a Pre-requisite for considering your quotations.

16.1 Financial Bid Format for Tier-1 (Basic Cloud Services)

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
A. Compute as Managed Service												
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730						
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
13			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
14			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
17			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
18			VM - 2 vCPU, 16GB RAM	Hourly	1	730						
19			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
20			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
21			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
22			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
23			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
24			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
25			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
26			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
28			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
29			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
30		Windows Standard edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730						
31			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
32			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
33			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
34			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
35			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
36			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR)	Total Monthly offered Cost in INR	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
37			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
39			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
40		Windows Datacenter edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730						
41			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
42			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
43			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
44			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
45			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
46			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
47			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
48			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
B. Storage as a Managed Service - Object, File and Block Storage												
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly						
2	Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly						
3	Managed Storage- SSD	Managed SSD Storage for Mission Critical Web, Apps & DB	Single SSD redundant volume from Storage tier which support single-digit millisecond latency without Disk Striping	1 GB Per Month	5	Monthly						
				10 GB Per Month	5	Monthly						
				100 GB Per Month	5	Monthly						
				500 GB Per Month	5	Monthly						
				1000 GB Per Month	5	Monthly						
				2000 GB Per Month	5	Monthly						

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR)	Total Monthly offered Cost in INR	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
				3000 GB Per Month	5	Monthly						
				4000 GB Per Month	5	Monthly						
				5000 GB Per Month	5	Monthly						
				10000 GB Per Month	5	Monthly						
C. CSP/MSP Managed DB - Managed services												
1	Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL/My-SQL as a service with automated backups and point-in-time recovery	2 vCPU 8 GB RAM	Hourly	2	730						
2			4 vCPU 16 GB RAM	Hourly	2	730						
3			8 vCPU 32 GB RAM	Hourly	2	730						
4			16 vCPU 64 GB RAM	Hourly	2	730						
5			32 vCPU 128 GB RAM	Hourly	2	730						
6			48 vCPU 192 GB RAM	Hourly	2	730						
7			64 vCPU 256 GB RAM	Hourly	2	730						
8			96 vCPU 384 GB RAM	Hourly	2	730						
D. Other Managed / Additional Services / Network / Back-up / Security												
1	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly						
2	Site to Site VPN - Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly						

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
3	Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly						
4	Managed TCP Load balancer (L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly						
5	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly						
6	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control, Backup activity monitoring	per TB / per month	1	Monthly						
7	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly						
8	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly						

S. No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
9	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly						
10	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly						
11	Managed DDoS Protection and WAF	Web Application Firewall as Managed service	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly						
12	Network Firewall - NGFW	Managed Network Firewall - IPDS NGFW	Managed Network Firewall with intrusion detection / prevention system with 4 Gbps throughput	Monthly	1	Monthly						
TOTAL												

16.2 Financial Bid Format for Tier-2 (Intermediate Cloud Services)

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
A. Compute as Managed Service												
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ [12]	CSP Public URL [13]
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
13			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
14			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
17			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
18			VM - 2 vCPU, 16GB RAM	Hourly	1	730						
19			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
20			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
21			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
22			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
23			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
24			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
25			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
26			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
28			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ [12]	CSP Public URL [13]
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
29		Windows Standard edition O/S with O/S Licenses	VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
30			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
31			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
32			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
33			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
34			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
35			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
36			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
37			VM - 80 vCPU, 320 GB RAM	Hourly	1	730						
38			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
39			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
40		Windows Datacentre edition O/S with O/S Licenses	VM - 2 vCPU, 8GB RAM	Hourly	1	730						
41			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
42			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
43			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
44			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
45			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
46			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
47			VM - 80 vCPU, 320 GB RAM	Hourly	1	730						
48			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
49			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
B. Storage as a Managed Service - Object, File and Block Storage												

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly						
2	Archive Storage	Managed Archival Storage	Fully Managed Geo Redundant Archival/ Cold Tier	TB per month	100	Monthly						
3	Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly						
4	Managed Storage- SSD	Managed SSD Storage for Mission Critical Web, Apps & DB	Single SSD redundant volume from Storage tier which support single-digit millisecond latency without Disk Striping	1 GB Per Month	5	Monthly						
				10 GB Per Month	5	Monthly						
				100 GB Per Month	5	Monthly						
				500 GB Per Month	5	Monthly						
				1000 GB Per Month	5	Monthly						
				2000 GB Per Month	5	Monthly						
				3000 GB Per Month	5	Monthly						
				4000 GB Per Month	5	Monthly						
				5000 GB Per Month	5	Monthly						
				10000 GB Per Month	5	Monthly						
C. CSP/MSP Managed DB - Managed services												
1	Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL/My-SQL as a service with following features: d) Automated backups and point-in-time recovery or equivalent e) Automatic Storage Increase f) Should support horizontal scaling by adding/removing read replicas.	2 vCPU 8 GB RAM	Hourly	2	730						
2			4 vCPU 16 GB RAM	Hourly	2	730						
3			8 vCPU 32 GB RAM	Hourly	2	730						
4			16 vCPU 64 GB RAM	Hourly	2	730						
5			32 vCPU 128 GB RAM	Hourly	2	730						
6			48 vCPU 96 GB RAM	Hourly	2	730						
7			64 vCPU 128 GB RAM	Hourly	2	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
8		Bidder must Quote the Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	96 vCPU 256 GB RAM	Hourly	2	730						
D. Other Managed / Additional Services/ Network / Back-up / Security												
1	Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100 GB/Month	1	Monthly						
2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support service mesh for observability, network and security.	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	1	730						
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly						
4	Site to Site VPN - Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly						
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	1	Monthly						
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100 Hrs/Per month	1	Monthly						
7	Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-	Per month	1	Monthly						

S.No. [1]	Service Name / Type of Service [2]	Configuration/Description of Service [3]	Specifications of required Service [4]	Unit of Measurement of Service [5]	Indicative unit(s) of Service in a month [6]	Total Indicative Hours in a Month / Billing Cycle [7]	Unit rate (CSP public pricing in INR) [8]	Offered Price in INR [9]	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ [12]	CSP Public URL [13]
			balancing traffic. Load Balancers with data being processed up to 1TB/month									
8	Managed TCP Load balancer(L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly						
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly						
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	1	Monthly						
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly						
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly						
13	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly						
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
16	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and get visibility of cloud assets and resources on single Dashboard	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed/month	10	Event/cloud operation per month						
17	Managed DdoS Protection and WAF	Web Application Firewall as Managed service	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly						
18	Network Firewall - NGFW	Managed Network Firewall - IPDS NGFW	Managed Network Firewall with intrusion detection / prevention system with 4 Gbps throughput	Monthly	1	Monthly						
E. Content Delivery Network (CDN)												
1	Managed Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	1	Monthly						
F. GPU As Service												
1	Production Grade Virtual Machine with GPU	GPU Config: FP32 - 30.3 teraFLOPs Or Above Configuration and GPU Memory- 24 GB/GPU or Above Configuration) with Virtual Machine Configuration	VM - 2 vCPU, 16GB RAM, 1 GPU	Hourly	1	730						
2			VM - 8 vCPU, 32GB RAM, 1 GPU	Hourly	1	730						
3			VM - 12 vCPU, 48GB RAM, 1 GPU	Hourly	1	730						
4			VM - 16 vCPU, 64GB RAM, 1 GPU	Hourly	1	730						
5			VM - 32 vCPU, 128GB RAM, 1 GPU	Hourly	1	730						
6			VM - 24 vCPU, 96GB RAM, 2 GPU	Hourly	1	730						
7			VM - 48 vCPU, 192GB RAM, 4 GPU	Hourly	1	730						
8			VM - 96 vCPU, 384 GB RAM, 8 GPU	Hourly	1	730						
TOTAL												

16.3 Financial Bid Format for Tier-3 (Advanced Cloud Services)

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
A. Compute as Managed Service												
1	Non burstable x86 architecture - Production Grade Virtual Machine	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
2			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
3			VM - 2 vCPU, 16GB RAM	Hourly	1	730						
4			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
5			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
6			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
7			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
8			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
9			VM - 32 vCPU, 128GB RAM	Hourly	1	730						
10			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
11			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
12			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
13			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
14		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Hourly	1	730						
15			VM - 2 vCPU, 8GB RAM	Hourly	1	730						
16			VM - 2 vCPU, 16GB RAM	Hourly	1	730						
17			VM - 4 vCPU, 8GB RAM	Hourly	1	730						
18			VM - 4 vCPU, 16GB RAM	Hourly	1	730						
19			VM - 4 vCPU, 32GB RAM	Hourly	1	730						
20			VM - 8 vCPU, 32GB RAM	Hourly	1	730						
21			VM - 16 vCPU, 64GB RAM	Hourly	1	730						
22			VM - 32 vCPU, 128GB RAM	Hourly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
23			VM - 48 vCPU, 192GB RAM	Hourly	1	730						
24			VM - 64 vCPU, 256 GB RAM	Hourly	1	730						
25			VM - 96 vCPU, 384 GB RAM	Hourly	1	730						
26			VM - 128 vCPU, 512 GB RAM	Hourly	1	730						
27		Windows Standard edition O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Hourly	1	100						
28			VM - 4 vCPU, 16GB RAM	Hourly	1	100						
29			VM - 8 vCPU, 32GB RAM	Hourly	1	100						
30			VM - 16 vCPU, 64GB RAM	Hourly	1	100						
31		** O/S Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding)	VM - 32 vCPU, 128GB RAM	Hourly	1	100						
32		Windows Datacenter edition O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Hourly	1	100						
33			VM - 4 vCPU, 16GB RAM	Hourly	1	100						
34			VM - 8 vCPU, 32GB RAM	Hourly	1	100						
35			VM - 16 vCPU, 64GB RAM	Hourly	1	100						
36		** O/S Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding)	VM - 32 vCPU, 128GB RAM	Hourly	1	100						
37	Function as a Service	Bidder must quote Serverless, event-driven compute service that let developers run code without provisioning or managing servers	1 GB RAM , Requests per month (millions) =1 and Average execution time per request (ms)= 1000 ms	Hourly	1	730						
38	Serverless Compute as a Service	Fully managed Serverless compute for containers: a) Linux Support	Serverless compute with 1 vCPU 4 GB RAM	Hourly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
39		b) OS updates c) underlying infrastructure d) dynamically scale capacity in response to changes in demand to reduce waste e) highly available	Serverless compute with 2 vCPU 8 GB RAM	Hourly	1	730						
B. Storage as a Managed Service - Object, File and Block Storage												
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	100	Monthly						
2	Archive Storage with milliseconds restore tier	Managed Archival Storage - Restored quickly in milliseconds	Fully Managed Geo Redundant Archival/ Cold Tier with instant restore time	TB per month	100	Monthly						
3	Cloud Native Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	1	Monthly						
4	Managed Storage- SSD	Managed SSD Storage for Mission Critical Web, Apps & Databases	Single SSD redundant volume from Storage tier which support Sub-millisecond latency performance.	1 GB Per Month	5	Monthly						
				10 GB Per Month	5	Monthly						
				100 GB Per Month	5	Monthly						
				500 GB Per Month	5	Monthly						
				1000 GB Per Month	5	Monthly						
				2000 GB Per Month	5	Monthly						
				3000 GB Per Month	5	Monthly						
				4000 GB Per Month	5	Monthly						
				5000 GB Per Month	5	Monthly						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ [12]	CSP Public URL [13]
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
				10000 GB Per Month	5	Monthly						
C. Managed DB - Native Managed services by CSP												
1	CSP Native Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas	2 vCPU 8 GB RAM	Hourly	2	730						
2			4 vCPU 16 GB RAM	Hourly	2	730						
3			8 vCPU 32 GB RAM	Hourly	2	730						
4			16 vCPU 64 GB RAM	Hourly	2	730						
5			32 vCPU 128 GB RAM	Hourly	2	730						
6			48 vCPU 96 GB RAM	Hourly	2	730						
7			64 vCPU 128 GB RAM	Hourly	2	730						
8		Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	96 vCPU 256 GB RAM	Hourly	2	730						
9		MS SQL Server 2017 / 2019 / 2022 Enterprise/Standard as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) MS-SQL Licenses as per proposed CSP native billing – PAYG Option (* No optimization for licenses, assuming existing BYOL, software assurance, Hybrid or equivalent benefits for price bidding)	2 vCPU 4 GB RAM	Hourly	1	100						
10			4 vCPU 8 GB RAM	Hourly	1	100						
11			8 vCPU 16 GB RAM	Hourly	1	100						
12			16 vCPU 32 GB RAM	Hourly	1	100						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
		Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing										
13	CSP Native Redis Cluster as Service - Production Grade supporting Sharding	Managed Redis as a Service with: - Should support the Managed Cache database service - Supports partitions/shards and read replicas - Must be compatible with open-source Redis data store - Inbuilt capability to auto-scale shards and read replicas - Shards data across Redis nodes	130 GB Enterprise Grade Redis with Sharding support	Monthly	2	Monthly						
14	Production Grade CSP Native Managed Non- Relational Database(NoSQL) as Managed Services	Scalable NoSQL DB as Managed Service 1) Automated replication/Automatic failover to another Zone and region 2)Automated Backup 3)Multi -AZs HA architecture	Storage (GB) - 50 , Number of writes / Second: 1000 , Number of reads / Second: 2000, Backup - 30 days	Monthly	2	Monthly						
D. Other CSP Managed / Additional Services / Network / Back-up / Security												
1	CSP native Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100GB/Month	1	Monthly						
2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
		service mesh for observability, network and security.										
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly						
4	Site to Site VPN - CSP Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1 Gbps bandwidth per VPN tunnel	Monthly	1	Monthly						
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	1	Monthly						
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100hrs/Per month	1	Monthly						
7	CSP Natively Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly						
8	CSP Natively Managed TCP Load balancer(L3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	1	Monthly						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	1	Monthly						
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	1	Monthly						
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	1	Monthly						
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	100	Monthly						
13	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	Monthly						
14	Messaging services	Should provide a managed message queueing service for communicating between decoupled application components	Standard queue requests and FIFO queue requests in millions /1GB Volume with number of Subscriptions per Month	Monthly	1	Monthly						
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	1	Monthly						
16	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed/month	10	Event/cloud operation per month						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
		get visibility of cloud assets and resources on single Dashboard										
17	Managed DdoS Protection and WAF	Web Application Firewall CSP Natively Managed	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	1	Monthly						
18	Network Firewall - Cloud Native NGFW	CSP Native Managed Network Firewall - IPDS NGFW with Transport Layer Security (TLS) interception and decryption	Managed Network Firewall with intrusion detection / prevention system. Each firewall endpoint will process 50 Terabyte of traffic /50 TB data processed per month , the Billing will be based on the actual consumption	Monthly	1	Monthly						
E. CSP Native Content Delivery Network (CDN)												
1	Managed CSP Native Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	1	Monthly						
F. CSP Native AI/ML & Data Warehouse Platform												
1	ML Notebook	Fully managed CSP native Notebook IDE - Fully Managed & collaborative Jupyter Notebook - to perform all ML development steps (Prepare, build, Train & Deploy) from a single Web based visual interface.	Node Size 16 vCPU 64 GB RAM	Monthly	2	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10] = [6]x [7]x [8]	[11] = [6] x [7] x [9]	[12]	[13]
2	ML Training	Fully managed CSP native Training Jobs Service: GPU-powered instances for running training jobs. One Node - (24vCPU, 96GB of memory, 2 Nos of GPUs that supports TensorFlow, PyTorch, XgBoost ML-API for training Models and network performance of 32 Gbps)	Node Size: 24vCPU, 96 GB RAM with 2 GPUs / training job per month/730hrs	Monthly	2	730						
3	ML Inference	Real Time Inference	Node Size 16 vCPU 64 GB RAM	Monthly	2	730						
4	Fully Managed Data Warehouse	Full managed Datawarehouse with - Cloud-based enterprise data warehouse (EDW) to run complex queries across petabytes of data.	Data Warehouse Platform: a. Cloud-based enterprise Data warehouse - each unit/node having minimum configuration of 4 vCPU & 32 GB RAM, for running complex Queries(Approximate 100 Queries in Month with each query scanning of minimum of 100GB of data with 4 dedicated nodes/units (1 leader node & 3 workers) for Number of units in estimated units with 100% utilization of dedicated nodes; Or b. Fully Managed Cloud-based Serverless data warehouse -should run complex queries (Approximate 100 Queries in Month with each query scanning	Monthly	1	730						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
			minimum of 100GB of data for Number of units in estimated units) Pls Note: Bidder to quote only one (either a or b) option, which must support HA cluster deployment & Data Governance features including Row level Security , Data Masking, and cluster encryption using Customer Managed Key									
5	Managed ETL as a Service	Managed ETL Service: - Serverless service to process and transfer data between different compute and storage services data sources at specified intervals, create, schedule, orchestrate and manage data pipelines	4vCPU and 16GB	Monthly	1	730						
6	Data Visualization /BI Service	Fully Managed Serverless service with - Auto-scalable - Data visualization service for telemetry data and operational metrics	Data Visualization Service	Monthly	1	730						
G. Generative AI As Service												
1	GenAI - Multimodal models/LLM Model hosted in India (As a service/hosted on CSP native AI Managed service)	Multimodal Managed large model API for Image, Video, Text & Audio	Image Input/image	million/Month	1	Monthly						
2			Video Input/second	1000000	1	Monthly						
3			Text Input & output – Token equivalent	million/Month	1	Monthly						
4			Audio Input/second	1000000	1	Monthly						

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Indicative unit(s) of Service in a month	Total Indicative Hours in a Month / Billing Cycle	Unit rate (CSP public pricing in INR)	Offered Price in INR	Total Monthly Cost (CSP public pricing in INR) [10] = [6]x [7]x [8]	Total Monthly offered Cost in INR [11] = [6] x [7] x [9]	Service Configuration Quoted in the BoQ	CSP Public URL
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]			[12]	[13]
H. GPU As Service												
1	Production Grade Virtual Machine with GPU	GPU Config: FP32 - 30 teraFLOPs Or Above Configuration and GPU Memory- 24 GB/GPU or Above Configuration) with Virtual Machine Configuration : Similar or higher as per Shape available on the CSP console	VM - 2 vCPU, 16GB RAM, 1 GPU	Hourly	1	730						
2			VM - 8 vCPU, 32GB RAM, 1 GPU	Hourly	1	730						
3			VM - 12 vCPU, 48GB RAM, 1 GPU	Hourly	1	730						
4			VM - 16 vCPU, 64GB RAM, 1 GPU	Hourly	1	730						
5			VM - 32 vCPU, 128GB RAM, 1 GPU	Hourly	1	730						
6			VM - 24 vCPU, 96GB RAM, 2 GPU	Hourly	1	730						
7			VM - 48 vCPU, 192GB RAM, 4 GPU	Hourly	1	730						
8			VM - 96 vCPU, 384 GB RAM, 8 GPU	Hourly	1	730						
9		GPU Config: FP32 - 60 teraFLOPs FP16 - 1600 teraFLOPs GPU Memory- 141 GB/GPU or Above Configuration with Multi-Instance GPUs MIGs support	VM - 192 vCPU, 2048 GB RAM with 8 GPUs	Hourly	1	100						
TOTAL												

Note:

- Item Unit Cost should be without Tax (GST). GST will be as per actuals.
- The Bidders are advised to quote rate in absolute Indian Rupees.
- Kindly do not enter DC + DR rates as only unit price is requested.
- Unit of Measurement of Service for Monthly is considered as a unit of 730 hours, and year will be 730 * 12.
- Unit of Measurement of Service is in TB/Month for Data transfer/Storage resources and may vary for different resources as mentioned in the table above.

- Bidder should provide an exhaustive list of services with specifications where 12-month trial can be availed and list of services which are usually provided Free of Cost by the Cloud Service Provider
- All the unit price mentioned for an item should be at discounted rate than the public listed price
- The bidder should provide the public price link for items quoted in BoM for All Cloud Services mentioned in "Financial Bid - Bill of Quantities".
- Submission of any pricing except public list prices of cloud services in the technical bid may lead to rejection of the bid.
- All the prices must be excluding any free tier benefits. For example, in case a service provides 1 TB data transfer out per month free of charge, and charges for additional incremental per TB data transfer over and above that, the bidder must quote prices of the item applicable over and above free tier benefit. If the bidder quotes price for any item as Zero ('0'), it will be treated as a zero-cost item throughout the contract period
- Bidders shall note that this RFE is aimed to discover the envisaged cloud services and rates thereof for quantities estimated basis current assessments. Actual consumption and quantities of cloud services may vary from the BoQ. And payments shall be made on actual items/services and quantities consumed during the contract period.
- The rate quoted will be reasonable and valid for the period of contract from the date of opening of financial Bid. The period can be extended with mutual agreement.
- No condition will be entertained, and conditional RFE will be liable to be rejected.

I/we hereby confirm that to the best of our knowledge and belief:

- 1) The rate quoted will be reasonable and valid for the period of 1 year from the date of opening of financial Bid. The period can be extended with mutual agreement.
- 2) RFE rates are at par with the prevailing market rates, and not more than the price usually charged for the same nature/class or description from any other, either foreign or as well as Government purchaser.
- 3) In respect of indigenous items/services for which there is a controlled price fixed by law, the price quoted is not higher than the controlled price.
- 4) Services/Products/Goods supplied, will be of requisite specification and quality.

Signature of the Bidder with stamp

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Place:

Date:

16.4 Financial Bid Format for Resources

(Mandatory for Bidders submitting in all categories: Tier-1, Tier-2 and Tier-3)

S. No.	Resource Profile with Experience level	Man-Month Rate of the Agency (in Rs. Without tax)		
		Level 1 (A) (Below 7 years)	Level 2 (B) (7 to 10 years)	Level 3 (C) (More than 10 years)
1	Project Manager (Cloud Services) · B.E. / B.Tech./MCA or equivalent · PMP or equivalent certification · Experience as Project Manager · Present experience in managing a Cloud- service project			
2	Solution Architect · B.E. / B.Tech. / MCA or equivalent · Experience in Solution Design			
3	Cloud Administrator · B.E. / B.Tech. / MCA or equivalent, · Experience in Implementation, Management and Operations			
4	System Administrator · B.E. / B.Tech. / MCA or equivalent, · Experience in Implementation, Management and Operations			
5	Network Administrator · B.E. / B.Tech. / MCA or equivalent, · Experience in network provisioning, configuration and management			
6	Security Administrator · B.E. / B.Tech. / MCA or equivalent			

	· Experience in Implementation, Management and Operations of security devices and solution			
7	DB Administrator · B.E. / B.Tech. / MCA or equivalent · Experience in database administration			
8	Storage / Backup expert · B.E. / B.Tech. / MCA or equivalent · Experience in managing storage, backup solutions, and disaster recovery			
9	Data Engineer / Science · B.E. / B.Tech. / MCA or equivalent · Experience in programming skills (Python, Java, SQL), knowledge of data structures, algorithms, and databases.			
TOTAL				
GRAND TOTAL (A + B + C)				

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

Note:

- For consideration of their bids, the bidders have to quote for all the resource levels. The rates quoted should be as per industry standards for the prescribed experience. For any of the resource levels, bids quoting zero or incredibly low rates compared to the industry prevalent rates will be rejected and execution of Bid Securing Declaration / Bid Securing Deposit.
- The rates finalized will not be changed throughout the period of empanelment/extended empanelment.
- GST and other taxes will be as per actuals.
- Prices should be quoted in Indian Rupee only.

ANNEXURE 17: Undertaking to Maintain KYC of Customers as per CERT-In Guidelines

<On Company's Letter Head>

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICS)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: **Undertaking for Maintenance of KYC Information of Customers**

We, [**Name of the Organization**], having our registered office at [**Address**], hereby undertake the following in compliance with the guidelines issued by the Indian Computer Emergency Response Team (CERT-In) under the provisions of the Information Technology Act, 2000:

1. **KYC Compliance:** We confirm that we have implemented a robust Know Your Customer (KYC) process for identifying and verifying all our customers/users in accordance with applicable laws and regulatory requirements.
2. **Retention of Information:** We undertake to maintain accurate and updated KYC information, including name, address, contact details, and other relevant identification details, of all our customers for a minimum period of **five (5) years** or as may be specified by CERT-In or any other competent authority, from the date of cessation of services to the customer.
3. **Availability for Audit/Inspection:** We agree to make such KYC records available to CERT-In and/or any designated authority upon lawful request for the purposes of audit, investigation, or cyber incident response.
4. **Data Protection:** We shall ensure that the KYC data is stored securely, protected from unauthorized access or tampering, and handled in accordance with applicable data protection and privacy laws.
5. **Responsibility and Compliance:** We accept full responsibility for ensuring continued compliance with CERT-In's directives, advisories, and guidelines as amended from time to time, particularly with regard to customer identification and KYC data management.

This undertaking is being submitted with full understanding of the obligations imposed under the CERT-In guidelines dated 28th April 2022 and any subsequent amendments thereto.

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 18: Undertaking by the CSP

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services

Ref: Bid No: <RFE Reference Number here>Dated <DD/MM/YYYY>

Dear Sir/ Madam,

We hereby confirm and declare that we, M/s,_____ have been empanelled by MeitY.

We further certify:

1. We have a running Government Community Cloud (GCC) / Virtual Private Cloud (VPC) service.
2. We are compliant with IT Act 2000 (including 43A) and amendments
3. The proposed Data Centre is in India.
4. Our services are operating in multiple Data Centres across India.
5. Our DC and DR Centres are in two different seismic zones in India
6. All the data that will be acquired and processed through the system will reside in India
7. We will provide the department the flexibility to create resources like Virtual instance, storage and other services of any configuration and not restrict to specific configuration.
8. We have a registered office in Delhi/NCR.
9. We are not subjected to any legal action for any cause in any legal jurisdiction in the last five years.

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

Enclosure:

- Required supporting documents
- Additional relevant and required documents if any

ANNEXURE 19: Undertaking by the MSP

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services

Ref: Bid No: <RFE Reference Number here>Dated <DD/MM/YYYY>

Dear Sir/ Madam,

We hereby confirm and certify that,

1. We are compliant with IT Act 2000 (including 43A) and amendments
2. All the data that will be acquired and processed through the system will reside in India
3. We will be the single point of responsibility by owning and providing Cloud services as requested.
4. We will provide the department the flexibility to create resources like Virtual instance, storage and other services of any configuration and not restrict to specific configuration.
5. We have a registered office in Delhi/NCR.
6. We are not subjected to any legal action for any cause in any legal jurisdiction in the last five years.
7. We have submitted the Earnest Money Deposit to the department.

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

Enclosure:

- *Required supporting documents*
- *Additional relevant and required documents if any*

ANNEXURE 20: Format for Non-Disclosure Agreement (NDA)

Non-Disclosure Agreement (NDA)

I, _____, on behalf of the _____ (Name of Company), acknowledge that the information received or generated, directly or indirectly, while working with NICSI/User department on contract is confidential and that the nature of the business of NICSI/User department is such that the following conditions are reasonable, and therefore: I warrant and agree as follows: I, or any other personnel employed or engaged by our company, agree not to disclose, directly or indirectly, any information related to the NICSI/User department. Without restricting the generality of the foregoing, it is agreed that we will not disclose such information consisting of but not necessarily limited to:

- Technical information: Methods, drawings, processes, formulae, compositions, systems, techniques, inventions, computer programs/data/configuration and research projects.
- Business information: Customer lists, project schedules, pricing data, estimates, financial or marketing data.

On conclusion of contract, I, or any other personnel employed or engaged by our company shall return to NICSI/User department all documents and property of NICSI/User department, including but not necessarily limited to drawings, blueprints, reports, manuals, computer programs/data/configuration, and all other materials and all copies thereof relating in any way to NICSI/User department business, or in any way obtained by me during the course of contract. I further agree that I, or any others employed or engaged by our company shall not retain copies, notes or abstracts of the foregoing.

This obligation of confidence shall continue after the conclusion of the contract also. I acknowledge that the aforesaid restrictions are necessary and fundamental to the business of the NICSI/User department and are reasonable given the nature of the business carried on by the NICSI/User department. I agree that this agreement shall be governed by and construed in accordance with the laws of country.

I enter into this agreement totally voluntarily, with full knowledge of its meaning, and without duress.

Dated at _____, this _____ day of, 20____.

Signature of the Bidder with stamp

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 21: Auditor's Certificate for Positive Net worth

<Declaration by the statutory auditor/CA >

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: "RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services"

Dear Sir,

This is to certify that the Net Worth of M/S..... <Registered name of bidder > as per books and records for the following financial years are as under.

#	Financial Year	Annual Net worth (in INR Crores)
1.	FY 2021-22	
2.	FY 2022-23	
3.	FY 2023-24	

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

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

ANNEXURE 22: Auditor's Certificate for Avg. Annual Turnover (CSP)

<Declaration by the statutory auditor/CA >

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: "RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services"

Dear Sir,

This is to certify that the Annual Turnover of M/S..... <Registered name of bidder > from the 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 2021-22	
2.	FY 2022-23	
3.	FY 2023-24	
Average Annual Turnover		

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

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

Instructions

1. The Bidder shall attach copies of the Balance Sheets and Profit & Loss Statements for the Financial Years 2021-22, 2022-23, 2023-24.

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).

ANNEXURE 23: Auditor's Certificate for Avg. Annual Turnover (MSP)

<Declaration by the statutory auditor/CA >

<Date>

To

The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066.

Subject: "RFE for Rate Empanelment of MSPs for Provisioning of Cloud Services"

Dear Sir,

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

#	Financial Year	Annual Turnover (in INR Crores)
1.	FY 2021-22	
2.	FY 2022-23	
3.	FY 2023-24	
Average Annual Turnover		

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

Yours sincerely,

On behalf of [bidder's name]

Authorized Signature [In full and initials]:

Name & Title of signatory:

Name of Firm:

Address:

Seal/Stamp of bidder:

Place:

Date:

Instructions

1. The Bidder shall attach copies of the Balance Sheets and Profit & Loss Statements for the Financial Years 2021-22, 2022-23, 2023-24.

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).