Name Of Organization submitting request			ESDS Software Solution Limited			
S.No.	**EoI Section & Clause No.**	**Page No.**	**Existing EoI Clause Text**	**Clarification / Relaxation Requested**	**Justification & Remarks**	**CDAC Comments**
1	Section II, Clause 2(iii) – Industries (Sl. No. 2: Operational Presence & Sl. No. 4: Proven Expertise)	13	*"Proven expertise in Cloud domain… demonstrating experience in developing, deploying, integrating, or managing cloud infrastructure, cloud platforms…"*	Clarification Requested: Can work experience gained from deploying and operating our own-operated and self-managed cloud Data Centres (DCs) be counted as valid qualifying experience for "similar work experience" or "proven expertise"?	As a MeitY-empanelled Cloud Service Provider (CSP), our own-operated Data Centres are fully compliant, audited, and certified under MeitY guidelines. Recognising self-managed DC operations ensures that partners with deep, end-to-end cloud infrastructure experience are eligible to participate.	Self-managed Cloud Data Centre operations and cloud services constitute as relevant cloud expertise, subject to evidence.
2	Chapter 3, Section III, Clause 4 – Modes of Engagement, sub-clauses (iv) and (v)	25	*(iv) "For each domain/category, one (01) eligible entity shall be selected based on the highest marks obtained…"* *(v) "C-DAC may onboard multiple entities in each domain depending on the uniqueness and applicability of their proposed solutions."*	Clarification Requested: Sub-clauses (iv) and (v) appear to conflict on whether one or multiple entities will be empanelled per domain/line item. Kindly clarify the objective criteria C-DAC will apply to decide when more than one entity is onboarded for the same domain.	Clarity on this point directly affects bidders' evaluation of competitive positioning and go/no-go decisions for specific cloud-service domains under Annexure-1.	For each cloud service/category, normally one (01) eligible entity obtaining the highest marks will be selected for empanelment. However, where two or more eligible entities obtain equal highest marks for the same cloud service/category, and their respective proposed solutions are found to be unique and applicable to the requirements of C-DAC,then C-DAC may empanel more than one entity for that cloud service/category. Accordingly, sub-clause (v) shall be applicable only in such circumstances and shall not be construed as permitting multiple entities to be empanelled where a single entity has obtained the highest marks.
3	Section II, Clause 2(iii) – Industries, Sl. No. 5 (Consortium Bid restriction)	13	*"Consortium Bid participation is not allowed under this RFP."*	Clarification Requested: Kindly clarify whether an Industry bidder may still propose a joint solution involving an OEM/technology-partner relationship (e.g., product OEM plus system integrator) that falls short of a formal consortium, and whether the no-consortium restriction also applies to the Startup and Academia categories.	The EoI is silent on Startup/Academia consortium eligibility, and many cloud-service line items (Annexure-1) require combined product + integration capability. Clarification will help bidders structure compliant proposals.	Eligible bidder may associate with an OEM/technology partner for providing the proposed cloud service or solution. The bidder shall submit the EOI independently and shall remain responsible for the proposed solution, integration, service delivery, and compliance with the requirements of the EOI.

4	Section II, Clause 4 – Evaluation Criteria, Sl. No. 6 (PoC/Product Demonstration – 25 marks)	14–15	*"Required to demonstrate their existing product (or) PoC demonstration relevant to the specified cloud service category."*	Clarification Requested: Kindly clarify (a) whether the PoC/product demonstration is to be conducted on the bidder's own environment or on C-DAC's Meghdoot staging infrastructure, and (b) for compute-intensive categories (AI/ML, Data Analytics), whether C-DAC will provision the requisite GPU/compute resources for the demonstration or whether bidders must arrange these independently.	This criterion carries the highest weightage (25 of 100 marks) in the technical evaluation. Clarity on the demonstration environment is essential for bidders to prepare adequately and ensures a level playing field.	For non-GPU/compute-intensive cloud services, the PoC shall be conducted in the C-DAC staging environment. For GPU/compute-intensive cloud services, the PoC may be conducted in the bidder's environment, provided that the Meghdoot Cloud Stack is first deployed on bare-metal hardware in the bidder's environment. The proposed GPU/compute-intensive cloud services shall subsequently be deployed and demonstrated on top of the Meghdoot Cloud Stack.
5	Section II, Clause 2(iii) – Industries, Sl. No. 6 (Financial Stability)	13	*"Financial Stability – Certificate by statutory auditor to be submitted" (no threshold specified)*	Clarification Requested: Kindly specify the minimum financial threshold (e.g., minimum annual turnover or net worth over the last 3 financial years) that the statutory auditor's certificate should confirm, if any is intended, so that bidders can prepare the appropriate certification.	Without a defined threshold, "financial stability" is open to subjective interpretation during evaluation, which could lead to inconsistent assessment across bidders.	**Refer Corrigendum 3**
6	Chapter 3, Section III, Clause 1 (Background) & Figure 1 – Meghdoot Cloud Suite Layer	21–23	*"Clusters will be on the Meghdoot Cloud suite (based on OpenStack) with KVM as default hypervisor and BOSS Linux as the base operating system…"*	Clarification Requested: Meghdoot's underlying stack is fixed to OpenStack, KVM, and BOSS Linux. Can a bidder propose a cloud service built on a different underlying technology stack (e.g., a different hypervisor, container runtime, or base OS) provided the resulting service integrates with Meghdoot at the API/portal level? Or must all proposed services be natively built on Meghdoot's OpenStack/KVM/BOSS Linux stack?	Several categories in Annexure-1 (e.g., AI/ML, Analytics, IoT) are commonly built on stacks that differ from OpenStack/KVM/BOSS Linux. Clarifying whether stack substitution is permitted — versus strict native integration — is essential for bidders to scope technical feasibility and effort before proposing a solution.	Meghdoot Cloud Suite is based on OpenStack and BOSS GNU/Linux, with C-DAC's in-house value additions. The proposed cloud services are not required to be natively built on the Meghdoot OpenStack/KVM/BOSS GNU/Linux stack. Services implemented using Kubernetes, container runtimes, or other appropriate underlying technologies may also be proposed, provided that they can be integrated with the Meghdoot Cloud Suite through appropriate APIs, interfaces, or integration mechanisms. The underlying Meghdoot Cloud Stack shall remain based on OpenStack, KVM, and BOSS GNU/Linux.

7	Chapter 3, Section III, Clause 1 (Background) – Components of the Cloud Middleware	22–23	*"The cloud management platform includes integrated software-defined storage and networking capabilities. It leverages Neutron…" and related OpenStack component descriptions (Compute, Networking, Identity, Image, Orchestration services)*	Clarification Requested: Can C-DAC share the detailed API/interoperability specifications (e.g., OpenStack API versions, Identity/Keystone integration method, Orchestration/HOT template compatibility) of the Meghdoot Cloud Suite, either during the pre-submission meeting or post-empanelment, so that bidders can accurately assess the integration effort and timelines referred to in Clause 5 (Post-Empanelment Integration Requirements)?	Clause 5 requires integration within 3–5 months of empanelment. Without visibility into the exact APIs/interfaces exposed by Meghdoot, bidders cannot reliably estimate integration effort or commit to these timelines at the proposal stage.	The bidder shall assess the integration requirements based on the Meghdoot Cloud Suite architecture and use the appropriate OpenStack APIs, tools, components, and interfaces required for integrating the proposed cloud service with Meghdoot. The detailed integration requirements and technical specifications, as applicable, shall be discussed during the post-empanelment integration stage.
8	Chapter 3, Section III, Clause 4 – Modes of Engagement, sub-clauses (iii) and (iv) / Annexure-1	25, 30–47	*(iii) "C-DAC shall engage eligible entities for each domain/line item as defined in this document."* *(iv) "For each domain/category, one (01) eligible entity shall be selected based on the highest marks obtained…"*	Clarification Requested: Annexure-1 lists services at two levels — broad Category (e.g., "AI/ML", "Security, Identity & Compliance") and individually named Cloud Service (e.g., "Generative AI Platform", "Threat Detection Service") within each Category. Kindly clarify whether the "one entity per domain" principle in Clause 4(iv) applies at the Category level or the individual Cloud Service Name level, and whether a single bidder may submit proposals (with separate PoC/product demonstrations) for multiple individual Cloud Services, including services within the same Category.	This directly affects how many services a bidder can realistically apply for in one EoI response and how PoC/demonstration effort (25 of 100 evaluation marks, per domain) should be planned and budgeted.	The selection principle applies to the individual Cloud Service Name, rather than only the broad service category.

ne Of Organization submitting requ			HCL Technologies			
1				We believe 1 Partner can submit EoI for multiple domains, and will technical evaluation be carried out separately for each domain?		Yes. A partner may submit an EOI for multiple domains. Each domain will be evaluated separately based on the applicable evaluation criteria.
2				Requesting C-DAC team to elaborate on the scope, duration, and evaluation parameters for the PoC? If a partner is participating in multiple domains, do we need to perform multiple POC's?		For each cloud service for which the bidder is empanelled, the bidder shall be required to demonstrate the PoC. The post-empanelment integration timeline shall be as follows: (a) for existing cloud services, integration with the Meghdoot Cloud Suite shall be completed within three (3) months from the date of empanelment; and (b) for new cloud services proposed to be developed after empanelment, development and integration with the Meghdoot Cloud Suite shall be completed within four (4) to five (5) months from the date of empanelment. Accordingly, where a bidder is empanelled for multiple cloud services, the PoC shall be demonstrated for each respective cloud service
3				Development Cost - At the empanelment and integration stage, how would be the cost of resources, infrastructure, software licences and development/PoC activities accomodated? Will it be a mutually agreed cost-sharing model?		No cost shall be borne by C-DAC towards development, integration, or PoC activities.
4				IP Related Clarification - If the partner deploy our own solutions, will the IP rights will be with the partner or Will it need to be transferred to CDAC?		Where the partner deploys its own solution, the intellectual property rights (IPR) associated with the solution shall remain with the partner.
5				Will the bidder retain ownership and commercialisation rights over its pre-existing platform/product components used for Meghdoot integration		Yes. The bidder shall retain ownership and commercialisation rights over its pre-existing platform/product components used for integration with Meghdoot.

6				Once an entity is empanelled for a specific service category, will project-specific opportunities be invited from all empanelled entities in that category, or can C-DAC directly shortlist a limited number of empanelled entities based on solution relevance?		Only entities empanelled for the specific cloud service(s) relevant to the project requirement will be invited to participate in the corresponding limited bid.
7				What would be the commercial model of operations once the partner is shortlished for emplanelment?		The commercial model after empanelment will be based on a revenue-sharing model.
Name Of Organization submitting request			**HCL Technologies**			
Sl No	**Technology Domain**		**Clarification**			**CDAC Comments**
1	General		We believe 1 Partner can submit EoI for multiple domains, and will technical evaluation be carried out separately for each domain?		Yes; evaluation will be domain-specific.	
2	General/Evaluation & POC		Requesting C-DAC team to elaborate on the scope, duration, and evaluation parameters for the PoC? If a partner is participating in multiple domains, do we need to perform multiple POC's?		The PoC/Product Demonstration will be conducted for the respective Cloud Service(s) proposed by the applicant. The 25 marks allocated for PoC/Product Demonstration will be assessed based on the number of relevant Cloud Services/domain successfully demonstrated. The PoC shall be conducted within a maximum period of 10 working days.	
3	Commercial		Development Cost - At the empanelment and integration stage, how would be the cost of resources, infrastructure, software licences and development/PoC activities accomodated? Will it be a mutually agreed cost-sharing model?		No Cost during integration or development phase	
4	Legal / IP Rights		IP Related Clarification - If the partner deploy our own solutions, will the IP rights will be with the partner or will it need to be transferred to CDAC?		IP rights will be with partner	
5	Legal / IP Rights		Will the bidder retain ownership and commercialisation rights over its pre-existing platform/product components used for Meghdoot integration		Yes	
6	General		Once an entity is empanelled for a specific service category, will project-specific opportunities be invited from all empanelled entities in that category, or can C-DAC directly shortlist a limited number of empanelled entities based on solution relevance?		CDAC will go for Limited tender of empanelled entities	
7	Container		Is supplier expected to enhance an existing Meghdoot Kubernetes platform or design and implement a new managed Kubernetes or enterprise container platform? Supplier also wants to confirm if CDAC has finalized container platform technology, If yes, please share the container platform technology name? If Meghdoot Kubernetes platform already exists, please share the existing architecture, Kubernetes distribution, versions and current capabilities?		The container orchestration technology adopted in Meghdoot is Kubernetes, with the target platform supporting Kubernetes version 1.35 or later.	

8	Container		Please specify the target deployment model for container platform deployment, such as private cloud, sovereign cloud, hybrid cloud etc. along with the number of K8s clusters, environments, worker nodes that needs to created or deployed ?	The container platform is intended to provide Kubernetes-based services to a broad range of clients in a service-oriented model, similar to a public cloud. The platform should support multiple deployment models, including private, sovereign, hybrid, and other cloud environments. The final number of clusters, environments, and worker nodes will be determined during deployment based on the client's specific requirements and available infrastructure capacity
9	Container		Please confirm the required services, including managed Kubernetes, container registry, application containerization, self-service provisioning, autoscaling, monitoring, backup, disaster recovery, service mesh and CI/CD, and clarify whether C-DAC expects onlycontainer platform implementation or container platform managed operations as well?	The platform supports connectivity to external container registries such as Docker Hub, from which container images can be pulled and deployed. It can also support an internal/private container image repository. The requirement is primarily for the implementation and enablement of the container platform and its associated services, including managed Kubernetes, container registry, application deployment, and self-service provisioning. Other capabilities such as autoscaling, monitoring, backup/DR, service mesh, and CI/CD will be supported based on client requirements. Managed operations are not mandatory at this stage and may be taken up based on the specific client requirements and agreed service model.
10	Container		Supplier understands that application containerization & on-boarding will be done by C-DAC's internal application teams, Is our understanding correct? If not, please clarify the scope & expectations around application onboarding and containerization?	C-DAC's internal application teams may handle application containerization and onboarding; however, the platform should provide the required capabilities and support for application onboarding and deployment. The exact scope of containerization and onboarding activities will be determined based on the specific client/application requirements.
11	General		For solutions spanning multiple domains (for example, AI/ML, Cloud Security, Kubernetes Platforms, DevSecOps, and Cloud Operations), can an integrated proposal be submitted and evaluated across multiple categories?	Yes. An integrated proposal covering multiple domains/categories may be submitted, where the proposed solution has interdependent capabilities across areas such as AI/ML, Cloud Security, Kubernetes Platforms, DevSecOps, and Cloud Operations. The proposal may be evaluated based on the overall solution capability as well as the requirements of the respective categories.
12	Scope of Services		Kindly clarify the expected prioritization and roadmap of the cloud service categories listed in Annexure-1 so that participating organizations can align their offerings with C-DAC's near-term and long-term requirements.	C-DAC has not predefined a fixed prioritization or implementation roadmap for the cloud service categories listed in Annexure-1. The priority and deployment of individual services will be determined based on client requirements, demand, and project-specific needs. Participating organizations are therefore expected to propose scalable and flexible solutions that can support both near-term and future requirements.
13	Meghdoot Platform Architecture		Kindly share the Meghdoot reference architecture, supported APIs, integration standards, development toolkit, and onboarding guidelines applicable for partner solutions.	The Meghdoot reference architecture provided in the EOI may be referred to for the overall platform architecture. The platform follows open standards and OpenStack/Kubernetes-compatible APIs wherever applicable, enabling integration with partner solutions.
14	Meghdoot Platform Architecture		Will C-DAC provide a sandbox, development, and staging environment for integration, testing, and validation of the proposed services?	C-DAC may provide sandbox/development and staging environments, subject to availability and project-specific requirements, for integration, testing, and validation. The detailed onboarding guidelines and integration requirements will be shared during the implementation/onboarding phase.

15	Cloud Platform Architecture		Kindly clarify the supported technology stack and standards for integration, including OpenStack, Kubernetes, security frameworks, identity services, monitoring, orchestration, and automation components.	The supported technology stack is primarily based on OpenStack and Kubernetes, along with applicable open-source standards and components for security, identity, monitoring, orchestration, and automation. Specific APIs, versions, toolkits, and integration interfaces will be provided based on the service/solution and integration requirements.
16	General		For technical evaluation, will a live product demonstration be mandatory, or will recorded demonstrations, existing deployments, and customer success stories also be considered?	For the EOI stage, bidders may demonstrate existing commercial/enterprise solutions, recorded demonstrations, existing deployments, and relevant customer success stories.
17	General		Kindly provide details regarding the expected duration, format, and assessment parameters for the technical presentation and PoC demonstration.	The requirement for a live demonstration, PoC, presentation format, duration, and detailed assessment parameters will be communicated by C-DAC during the subsequent technical evaluation stage, as applicable.
18	General		Please confirm if bidders can demonstrate existing commercial or enterprise cloud solutions, or is a Meghdoot-integrated PoC expected during the EOI stage itself?	Yes, bidders can demonstrate existing commercial or enterprise cloud solutions
19	Commercial		Kindly indicate the anticipated engagement models for future projects, such as Fixed Price, Time & Material, Outcome-Based, Revenue Sharing, or Co-Development arrangements.	Revenue Sharing Engagement/Co Development
20	General		Are there any indicative project sizes, demand forecasts, or target customer segments envisaged under this initiative?	There are no predefined project sizes or demand forecasts at this stage. The initiative is intended to cater to varied customer segments and requirements
21	Security, Identity & Compliance		Kindly clarify whether compliance with standards such as CERT-In, STQC, ISO 27001, NCIIPC, MeitY guidelines, or other Sovereign Cloud requirements will be mandatory for empaneled partners.	Applicable standards will be project-specific.
22	Security, Identity & Compliance		Please confirm the data residency, sovereign hosting, and security requirements applicable to services proposed under this EOI.	Applicable requirements will be project-specific.
23	Security, Identity & Compliance		Will future projects under this program include requirements related to Community Cloud, Air-Gapped Environments, or Classified/Restricted Government workloads?	depends on the Project requirement
24	Networking & Connectivity		What is the current network architecture (LAN, WAN, SD-WAN, traditional Networks)?	Details will be shared as applicable.
25	Networking & Connectivity		What are the existing OEMs deployed (Cisco, Juniper, Nokia, HPE Aruba, Huawei, etc.) with each stack such as SDWAN, SDLAN and DCLAN ?	Details will be shared as applicable.
26	Networking & Connectivity		What is the current network topology?	Details will be shared as applicable.
27	Networking & Connectivity		What are the major performance challenges in the current network?	Details will be shared as applicable.
28	Monitoring & Observability		What monitoring and observability tools are deployed?	depends on the Project requirement

29	Automation		Please confirm automation tools that are currently being used?	Automation is currently carried out using Ansible for infrastructure provisioning, configuration management, and deployment activities. Kubernetes and associated tools are used for container orchestration and application lifecycle automation. Where applicable, CI/CD tools such as Jenkins/Argo CD are used for application deployment and Git-based automation.
30	Networking & Connectivity		How are sites connected today?	Details will be shared as applicable.
31	Networking & Connectivity		MPLS, SD-WAN, Satellite, Radio, Microwave, Fiber, or Hybrid?	To be finalized based on requirements.
32	Satellite Comunication		Please confirm if satellite communication integration is required?	depends on the Project requirement
33	Infrastructure Services		Please confirm the number of primary and DR data centers?	depends on the Project requirement
34	Networking & Connectivity		Which third-party systems must integrate with the network? Please share full details	To be finalized based on requirements.
35	Cybersecurity - GRC		Supplier requests clarification on the applicable regulatory and sovereignty frameworks expected to be supported (e.g., DPDP, CERT-In, MeitY policies, data residency requirements, sector-specific regulations), along with the number of compliance obligations currently being tracked.	The proposed GRC services shall support applicable Government of India policies, regulations, standards and guidelines relevant to the respective use case. Specific compliance requirements shall be finalized based on project requirements.
36	Cybersecurity - GRC		Supplier requests clarification on whether third-party service providers, hyperscalers, technology partners, or sub-processors are within scope for sovereignty and compliance assessments. If yes, kindly provide the expected number of vendors to be assessed annually.	The proposed cloud services are intended to support the objectives of the Sovereign Cloud ecosystem. Accordingly, the proposed service, including its underlying product/platform and associated third-party service providers, OEMs, Hyperscalers, Technology partners or Sub-processors, shall be assessed, where applicable, with respect to Indian ownership/control, data sovereignty, security, regulatory compliance and applicable Government of India requirements. The number will be based on the actual vendors onboarded/used during the year
37	Cybersecurity - GRC		Supplier requests clarification on the tools currently used for compliance management, audit management, risk management, evidence management, and reporting, and whether supplier support is expected for administration, operation, or governance of these platforms.	CDAC does not mandate integration with any specific existing compliance, audit, risk or evidence-management platform. The requirement for administration, operation or governance support, if applicable, shall be defined based on the specific service and project requirements.
38	Networking & Connectivity		Is the expectation to provide Authoritative DNS, Recursive DNS, or both?	DNS scope will be project-specific.
39	Networking & Connectivity		Will DNS be offered as a managed service for Meghdoot tenants, or only for Meghdoot platform administration?	Service model will be project-specific.
40	Networking & Connectivity		Are both public DNS zones and private/internal DNS zones required?	DNS zone requirements will be project-specific.
41	Networking & Connectivity		Is support required for DNSSEC and signed zones?	DNSSEC requirements will be project-specific.
42	Networking & Connectivity		Is IPv6 support mandatory (AAAA records, reverse DNS for IPv6)?	IPv6 requirements will be project-specific.
43	Networking & Connectivity		Should the service support automated DNS lifecycle management through APIs and self-service portal integration with Meghdoot?	API integration will be project-specific.

44	Networking & Connectivity		Are load-balancing/GSLB capabilities expected as part of DNS service?	GSLB requirements will be project-specific.
45	Security & Network		Is integration required with IAM/SSO for DNS administration?	depends on the Project requirement
46	Security & Network		Are audit logging, RBAC, and compliance reporting mandatory for DNS operations?	depends on the Project requirement
47	Networking & Connectivity		Should DNS service be deployed only in C-DAC staging initially and later productionized?	To be finalized based on requirements.
48	Networking & Connectivity		Are there any preferred open-source DNS technologies (BIND, PowerDNS, Knot DNS, CoreDNS, etc.) for Meghdoot integration?	To be finalized based on requirements.
49	Cybersecurity - IAM		Please confirm whether Access Governance capabilities such as access requests, role management, access certifications, Segregation of Duties (SoD), and compliance reporting are expected as part of the Identity Services offering.	The proposed Identity Services may include access governance capabilities such as access requests, role management, access certification, segregation of duties and compliance reporting, as applicable to the proposed service. The detailed functional requirements shall be finalized during the integration process.
50	Cybersecurity - IAM		Please provide details of the target authentication and federation ecosystem, including enterprise directories, external Identity Providers, government authentication services, and federation protocols expected to be supported.	The proposed Identity Services shall support appropriate authentication and federation mechanisms required for integration with the Meghdoot Cloud Suite. The specific identity providers, directories, federation protocols and authentication requirements shall be finalized based on the applicable service and project requirements.
51	Cybersecurity - IAM		Please provide the expected scope and volumetrics for Secrets Management, Certificate Management, Encryption Key Management, and HSM services, including lifecycle and rotation requirements.	The EOI does not prescribe fixed volumetrics or lifecycle/rotation parameters for these services. The capacity, lifecycle management and rotation requirements shall be determined based on the proposed service and project-specific requirements.
52	Cybersecurity - IAM		The EOI references IAM, Secrets Management, and Zero Trust Access capabilities. Please confirm whether Privileged Access Management (PAM) services are also expected and provide details regarding privileged accounts, credential vaulting, session monitoring, and privileged access governance requirements.	Privileged Access Management capabilities may be proposed as part of the Security, Identity & Compliance services, where relevant to the proposed solution. The specific requirements relating to privileged accounts, credential management, session monitoring and governance shall be finalized based on the applicable service and project requirements.
53	Analytics and Big Data		For the Analytics & Big Data category, are there any specific service areas or use cases that C-DAC considers strategic priorities for initial onboarding within the Meghdoot ecosystem?	The EoI does not prescribe specific priority use cases for initial onboarding. Applicants may propose Analytics and Big Data services relevant to the objectives and scope of the EoI, which will be evaluated based on their applicability and integration potential with the Meghdoot Cloud Suite.
54	Analytics and Big Data		Are there any technology, interoperability, security, or open-source compliance requirements that proposed Analytics & Big Data services should adhere to for Meghdoot integration?	The proposed services shall comply with applicable security, interoperability, and integration requirements of the Meghdoot Cloud Suite. The EoI does not mandate a specific technology stack or open-source framework; appropriate technologies may be proposed based on the nature of the service.
55	Application Integration		Can C-DAC provide additional guidance on the expected integration scope between proposed services and the Meghdoot platform at the EOI stage?	At the EoI stage, applicants are expected to provide an overview of the proposed service. CDAC will be provide the additional guidance during integration stage.

56	Application Integration		Are there any priority integration scenarios or target user segments that participants should consider while proposing Application Integration services?	CDAC does not prescribe specific priority integration scenarios or target user segments. Applicants may propose Application Integration services based on their existing capabilities and their applicability to the Meghdoot Cloud ecosystem.
57	Blockchain		Are there any priority sovereign cloud, digital governance, or enterprise scenarios that C-DAC intends to address through Blockchain services within Meghdoot?	CDAC does not prescribe specific priority use cases for Blockchain services. Applicants may propose relevant Blockchain capabilities applicable to sovereign cloud, digital governance, enterprise, or other suitable use cases within the scope of the EoI.
58	Business Applications		Can organizations propose mature SaaS/business application offerings for Meghdoot integration, or is the emphasis on joint development of new capabilities?	Yes, Bidder can propose mature application to be intergate with Meghdoot cloud stack
59	Cybersecurity Scope & Coverage		Please confirm the specific 'Security, Identity & Compliance' cloud service line items (from the ~24 listed in Annexure-1) that C-DAC intends to prioritize for co-development in Phase 1, versus items planned for later phases.	The EOI does not prescribe a fixed Phase-1 priority list for Security, Identity & Compliance services. Eligible entities may propose services listed under the relevant category based on their capabilities and applicability to the Meghdoot Cloud ecosystem. The specific services to be taken up shall be determined based on C-DAC's requirements.
60	Cybersecurity Scope & Coverage		For 'Identity Federation Service', 'Single Sign-On' and 'Directory Integration', should the proposed solution integrate natively with Meghdoot's existing OpenStack Identity Service (Keystone), or is a net-new, OpenStack-independent IAM stack expected?	The proposed Identity Services shall be capable of integration with the Meghdoot Cloud Suite and its existing identity and access-management components, as applicable. The specific integration architecture and interfaces shall be finalized during the post-empanelment integration process.
61	Cybersecurity Scope & Coverage		Does C-DAC expect the Hardware Security Module (HSM) service to be delivered via physical/dedicated HSM appliances hosted at the C-DAC Data Centre, or is a virtual/software HSM (FIPS 140-2/3 validated) acceptable given the Sovereign Cloud context?	CDAC does not prescribe a specific HSM deployment model at this stage. Eligible entities may propose appropriate HSM solutions, subject to applicable security, integration, performance and project requirements. The final deployment model shall be determined based on the specific project requirements.
62	Cybersecurity Scope & Coverage		Are the WAF, Network Firewall, and Bot Protection services expected to protect (a) tenant workloads hosted on Meghdoot, (b) the Meghdoot management/control plane itself, or (c) both?	The proposed security services may be applicable to tenant workloads, Meghdoot platform components, or both, depending on the specific service and security requirements. The applicable protection scope shall be finalized based on the project requirements.
63	Cybersecurity Scope & Coverage		What is the expected DDoS protection scope - Layer 3/4 (network volumetric) only, or Layer 7 (application-layer) as well? Is there an existing upstream/ISP-level DDoS scrubbing arrangement at the C-DAC Data Centre that the proposed service must integrate with?	The EOI does not prescribe a specific DDoS protection layer or upstream scrubbing architecture. Applicants may propose appropriate DDoS protection capabilities covering relevant network and application layers, subject to the requirements of the Meghdoot environment and the specific project.
64	Cybersecurity Scope & Coverage		Please clarify whether the Security Data Lake and Data Classification services are expected to ingest logs/telemetry only from Meghdoot-hosted workloads, or also from C-DAC's broader IT estate (non-cloud systems).	The scope of data ingestion is majorly from the Meghdoot-hosted workloads only.
65	Cybersecurity Scope & Coverage		Is a 24x7 Security Operations Centre (SOC) service (monitoring, triage, incident response) expected to be delivered as part of the co-developed Threat Detection/Security Investigation Platform capability, or is C-DAC only seeking the underlying software/platform to be built and integrated, with SOC operations handled separately by C-DAC or another partner?	Yes, it is Co-development. Applicants may propose SOC-related monitoring, detection, investigation and response capabilities solution where relevant to the proposed Security, Identity & Compliance service.

66	Cybersecurity Scope & Coverage		Will the Vulnerability Assessment and Security Posture Management services need to cover only the Meghdoot control plane and tenant VMs/containers, or also the underlying BOSS Linux/OpenStack hypervisor layer and physical infrastructure?	The Vulnerability Assessment and Security Posture Management services are expected to cover the relevant security layers of the Meghdoot Cloud environment, including the cloud control plane, tenant workloads (VMs/containers), and underlying platform components such as BOSS Linux, OpenStack and hypervisor layers, as applicable to the proposed service. The VAPT assessment shall be performed through appropriate and controlled access mechanisms by C-DAC.
67	Cybersecurity Scope & Coverage		Does C-DAC expect the proposed Secrets Management and Encryption Key Management services to replace/extend OpenStack Barbican, or to operate as an independent layer above it for application-level secrets used by tenants?	The proposed Secrets Management and Encryption Key Management services may integrate with existing Meghdoot/OpenStack components, where applicable. The specific integration or extension approach shall be finalized based on the proposed solution and technical requirements during the integration process.
68	Cybersecurity Scope & Coverage		For the Cybersecurity domain specifically, which of the indicative deliverables listed (System Design, HLD/LLD, SRS, Source Code with documentation, Requirement Traceability Matrix) are mandatory at the EoI/empanelment stage versus deliverables expected only after a specific Work Order is issued?	The deliverables specified in the EOI are indicative and relate to activities undertaken after selection/empanelment, as applicable. Detailed deliverables, including system design, HLD/LLD, SRS, source code, documentation and requirement traceability, shall be finalized based on the specific scope of work and project requirements.
69	Cybersecurity Integration Architecture		Please share the current security architecture/reference diagram of Meghdoot (identity, network security groups, DVR, VXLAN overlay) so that the proposed Security, Identity & Compliance services can be designed for compatibility with existing components (Neutron security groups, DMZ zone support, etc.) instead of being requested as post-EoI due diligence only.	The EOI provides the relevant high-level architecture and technical information required for bidders to understand the Meghdoot Cloud Suite. Detailed architecture, interfaces and integration information required for implementation shall be shared with the selected/empanelled entity, as applicable, during the post-empanelment integration process.
70	Cybersecurity Integration Architecture		What security framework/tools (if any) are already implemented within Meghdoot today (e.g., existing IDS/IPS, SIEM, key management) that the proposed Security, Identity & Compliance services must interoperate with or replace?	Currently, C-DAC does not have any specific security tools, such as SIEM, IDS/IPS or dedicated key management solutions, mandated for integration with the Meghdoot Cloud Suite. C-DAC is planning to implement a SIEM solution as part of its security architecture. Accordingly, the proposed Security, Identity & Compliance services should be capable of interoperating with the security framework and tools implemented or planned for Meghdoot, as applicable.
71	Cybersecurity Integration Architecture		For the Cybersecurity domain, will C-DAC engage a single empanelled entity for the entire 'Security, Identity & Compliance' category, or will individual line items (e.g., WAF vs. IAM vs. HSM) be separately empanelled to different entities/System Integrators as per Section 4(iv)?	Empanelment shall be considered at the individual Cloud Service Name level. An eligible entity may submit proposals for multiple individual cloud services, including multiple services within the Security, Identity & Compliance category, subject to meeting the applicable eligibility and evaluation requirements. An eligible bidder can submit a single proposal for multiple individual cloud services.
72	Cybersecurity Integration Architecture		Can HCLTech propose co-development of Cybersecurity services in partnership with an existing System Integrator/OEM security product vendor, and if so, how should such a partnership be represented in the EoI response (given Sec 3(iii) of Section II states 'Consortium Bid participation is not allowed')?	Consortium participation is not permitted under this EOI. However, an eligible participant may associate with an OEM/technology partner for providing the proposed cloud service or solution. The participant shall submit the EOI independently and remain responsible for the proposed solution, integration, service delivery and compliance with the EOI requirements. Such association shall not be construed as consortium participation.

73	Cybersecurity Integration Architecture		What compute/network resources (VMs, dedicated tenancy, network segment access) will C-DAC provision at the Data Centre staging environment for security-services PoC/demonstration and integration testing, and by when will this be made available post-empanelment?	The specific compute, network, access and other resources required for the PoC and integration shall be identified and provisioned based on the requirements and the exact resource sizing and network access requirements will be finalized jointly
74	Cybersecurity Data Sovereignty & Compliance		Are there specific Government of India security certification/empanelment prerequisites (e.g., CERT-In empanelment for security auditors, MeitY STQC certification, GIGW compliance) that a partner must hold or acquire to co-develop and operate the Cybersecurity services on a Sovereign Cloud platform?	CDAC does not prescribe a blanket certification or empanelment requirement for all Cybersecurity services. Where any specific certification, accreditation or Government of India requirement is applicable to the proposed service or project, the same shall be complied with as per the applicable requirements.
75	Cybersecurity Data Sovereignty & Compliance		For the Encryption Key Management, HSM, and Secrets Management services, is there a requirement that cryptographic modules/algorithms used be indigenously developed or approved under any GoI-notified list (e.g., NIC/MeitY approved cryptographic libraries), or are internationally certified (FIPS 140-2/3, Common Criteria) modules acceptable?	CDAC does not prescribe a specific cryptographic technology, algorithm, or certification at the EOI stage. Proposed solutions shall comply with applicable security and regulatory requirements. Specific cryptographic and certification requirements, where applicable, shall be determined based on the service and project requirements.
76	Cybersecurity Data Sovereignty & Compliance		For 'Proven expertise in Cloud domain' (Industries Eligibility, Sr. No. 4), will prior experience in delivering IAM/PAM/SIEM/WAF/HSM-based security services specifically (as opposed to general cloud infrastructure experience) be treated as a distinct, weighted qualifying criterion for the Cybersecurity domain, or is generic cloud experience sufficient?	Proven expertise in the Cloud domain shall be demonstrated as specified under the applicable eligibility criteria. Relevant experience in Cybersecurity services such as IAM, SIEM, WAF, HSM and related cloud security services may be considered as part of the assessment of the bidder's technical capability and domain expertise, where relevant to the proposed service.
77	Cybersecurity Technical Architecture		Given Meghdoot supports both KVM and Docker Containers as hypervisor/runtime options, should the proposed Security, Identity & Compliance services (e.g., Threat Detection, Vulnerability Assessment) support agent-based monitoring across both VM and container workloads, or is container-native (e.g., Kubernetes-aware) security tooling explicitly required?	The proposed Security, Identity & Compliance services should support the applicable workload environments of the Meghdoot Cloud Suite. Where the proposed service is intended to secure both VM and container workloads, the bidder shall clearly indicate the applicable monitoring, detection and security capabilities for each environment.
78	Cybersecurity Technical Architecture		For workloads running on the Meghdoot Container Service (Kubernetes-based), is Cloud-Native Application Protection (CNAPP)/Kubernetes security posture management explicitly expected as part of the Cybersecurity scope, or is it out of scope for this EoI?	CDAC does not mandate CNAPP or Kubernetes-specific security posture management as a separate requirement. Applicants may propose such capabilities where relevant to the proposed service and Meghdoot container environment, subject to the applicable technical and functional requirements.
79	Cybersecurity Technical Architecture		Are the Security, Identity & Compliance solutions required to be OS-agnostic, or is native compatibility/certification with BOSS Linux (Debian-based) specifically mandated, given Meghdoot is co-engineered with BOSS Linux?	For Co-development, OS agnostic is required and it is mandated.
80	Cybersecurity Technical Architecture		Please clarify whether 'Authorization Management' refers to fine-grained application-level RBAC/ABAC for tenant applications, or infrastructure-level authorization (e.g., cloud resource policies similar to AWS IAM policies) for the Meghdoot control plane.	The detailed authorization model and integration requirements shall be finalized based on the specific service and project requirements during the integration process.
81	Cybersecurity Technical Architecture		Are the Compliance Documentation Platform and Audit Management Service expected to map to specific Indian regulatory/compliance frameworks (e.g., MeitY guidelines, CERT-In directions, RBI/SEBI where applicable for future tenants), and should the platform pre-load these frameworks as templates?	Yes

82	Cybersecurity Technical Architecture		What API/interoperability standards (e.g., OpenStack-native APIs, REST, SAML/OIDC, Kubernetes CRDs) must the proposed security services expose to integrate with the Meghdoot Dashboard (self-service portal) referenced in Section 1?	The specific interoperability and integration requirements shall be discussed and finalized with the empanelled entity based on the proposed service and its technical architecture.
83	Cybersecurity Testing & Assurance		Is Vulnerability Assessment and Penetration Testing (VAPT) of the co-developed Security, Identity & Compliance services themselves (i.e., testing the security tooling for its own security posture) an in-scope deliverable, and if so, will C-DAC conduct this independently or expect the empanelled partner to provide VAPT reports as part of acceptance?	Yes, for the proposed security services CDAC will provide relevant security assessment/VAPT reports or supporting evidence as part of the applicable acceptance and assurance process to the empanelled entity.
84	Cybersecurity Support Model		For security services requiring privileged access (IAM, PAM, HSM, SIEM administration), what personnel security clearance/background-verification requirements (if any) will C-DAC mandate for HCLTech resources deployed on this engagement?	Personnel requiring access to C-DAC infrastructure, systems, or data shall comply with the applicable security, access-control, and background-verification requirements prescribed by C-DAC from time to time.
85	Cybersecurity Technology Roadmap		Does C-DAC have a preferred/mandated list of open-source security tools/frameworks (in line with the NRCFOSS/FOSS objective of Meghdoot) that must be used or evaluated first for the Security, Identity & Compliance services, before proprietary/commercial alternatives are considered?	Yes, C-DAC gives preferential consideration to open-source security tools and frameworks across key security domains, including OS Hardening, SIEM,PKI & Observability.
86	Cybersecurity Technology Roadmap		Will AI/ML-based capabilities (referenced under the separate 'AI & ML Services' category in Annexure-1) be expected to be integrated with the Security, Identity & Compliance services (e.g., AI-driven anomaly detection, UEBA) as part of this EoI, or is that cross-category integration out of scope at this stage?	Out of Scope
87	Cybersecurity Technology Roadmap		Please clarify the intended functionality of the 'Resource Sharing Service' listed under Security, Identity & Compliance - is this intended as cross-account/cross-tenant resource sharing with security guardrails (similar to AWS RAM), and if so, what cross-tenant isolation guarantees are required on Meghdoot's multi-tenant architecture?	Yes,The Resource Sharing Service is intended to enable controlled and secure sharing of cloud resources similar to AWS RAM.
88	Cybersecurity Technology Roadmap		Beyond the 24 listed Annexure-1 line items, is C-DAC open to partners proposing additional/emerging Cybersecurity capabilities not explicitly listed (e.g., Cloud Security Posture Management/CSPM, Secure Access Service Edge/SASE, Zero Trust Network Access) as part of the response, given Section 3 states the list is 'not limited to' the items shown?	Yes. The EoI scope is indicative and not limited to the cloud services listed in Annexure-1. Applicants may propose additional or emerging cybersecurity capabilities that are relevant to the objectives of the EoI and can be integrated with the Meghdoot Cloud Suite
89	Database		Does this scope include the database migration from source to target[Meghdoot Cloud]. If yes please provide the count and database technologies to migrated to Target.	Yes, depends on the Project requirement
90	Database		Please share the current database architetcure blue prints for HADR, Replication if implemented and need to be maintained on target cloud.	The current database architecture blueprints for High Availability (HA), Disaster Recovery (DR) and replication, wherever implemented, may be shared, as applicable, during the subsequent implementation phase. Existing database services include MySQL, PostgreSQL, MongoDB, MariaDB and BharatDB

91	Database		Does this scope include the Hetregeneous migration like oracle to PostgreSQL or any other such migrations.	Heterogeneous database migration, such as Oracle to PostgreSQL or other cross-database migrations, is not a mandatory predefined scope. Such migration requirements may be considered based on specific client/application requirements and the agreed scope of the project.
92	Private 5G and Private Cellular network (Neutral host)		Deployment scope and responsibility - Please clarify the expected end-to-end deployment scope for Private LTE/5G and Neutral Host solutions, including responsibility for RF planning and design, spectrum or regulatory coordination, site surveys, RAN, core and edge deployment, transport integration, indoor/outdoor coverage, testing, commissioning, acceptance, and integration with the Meghdoot Cloud Suite.	The deployment scope for Private LTE/5G and Neutral Host solutions will be determined based on the specific client/project requirements. The selected partner may be required to provide end-to-end support covering RF planning, site survey, RAN, core and edge deployment, transport integration, coverage, testing, commissioning, acceptance, and integration with the Meghdoot Cloud Suite, as applicable. Spectrum allocation and statutory/regulatory approvals will be subject to the applicable regulatory framework and client responsibilities. The detailed roles, responsibilities, deliverables, and acceptance criteria will be finalized during the implementation phase.
93	Private 5G and Private Cellular network (Neutral host)		Target architecture and neutral-host operating model - Please specify the intended deployment and tenancy model, such as enterprise-dedicated Private LTE/5G, MOCN/MORAN-based Neutral Host, or another model, and clarify which components (if any) must be shared or dedicated across tenants/operators, including RAN, core, spectrum, transport, edge cloud, OSS/NMS, security, and subscriber management.	No single deployment or tenancy model, such as enterprise-dedicated Private LTE/5G, MOCN, or MORAN, is predefined at this stage. The architecture and operating model will be determined based on the specific client, use case, regulatory, and service requirements. The solution should support flexible shared and/or dedicated deployment of RAN, core, spectrum, transport, edge cloud, OSS/NMS, security, and subscriber-management components, as applicable.
94	Private 5G and Private Cellular network (Neutral host)		Operations and managed-services coverage - Please confirm the required managed-services scope after deployment, including service desk, 24x7 monitoring, incident/problem/change management, configuration and performance management, fault isolation, software upgrades and patching, backup and recovery, capacity optimization, security operations, field maintenance, spares/RMA management, and coordination with OEMs, telecom operators, and site owners.	Scope will be defined project-wise.
95	EUC		HCLtech wishes to understand that the described Virtual Machine is of user PC or of cloud servers ?	The Virtual Machine referred to in the EOI is a cloud infrastructure VM provisioned on the Meghdoot Cloud platform, and does not refer to the user's physical PC or desktop system.
96	AI & ML		Please define the way AI based voice to text, and vice versa will be used and for which services.	The AI-based voice-to-text and text-to-voice capabilities are intended to support voice-enabled access to cloud services and applications, including virtual assistants, service requests, and other client-specific use cases.
97	AI & ML		Vendor wishes to understand more on Conversational AI usage and the chatbot using Natural Language.	Conversational AI/Natural Language chatbots may be used to provide natural-language interaction with cloud services, self-service portals, support/helpdesk, service provisioning, monitoring, and other client-specific applications. The exact use cases and scope will be determined based on the service and client requirements.

98	Media		Could C-DAC share the primary business objectives and target customer segments for the proposed Media Services portfolio, and whether the focus is on government broadcasters, OTT platforms, educational content providers, enterprise media organizations, individual content creators or a broader sovereign digital media ecosystem?	The Media Services portfolio is intended to support the broader sovereign cloud ecosystem by enabling media processing, delivery, and related cloud-based capabilities.
99	Media		Can C-DAC clarify whether the envisioned Media Services are intended to be offered as independently consumable cloud services or as components of a larger integrated Sovereign Media Cloud platform available through Meghdoot?	Service delivery model will be project-specific.
100	Media		Can C-DAC provide additional details regarding the reference architecture, integration framework, APIs, SDKs, and onboarding mechanisms available within the Meghdoot platform for incorporating third-party media services and applications?	The Meghdoot reference architecture provided in the EOI may be referred to for the overall platform architecture. Meghdoot follows open standards and OpenStack/Kubernetes-compatible APIs wherever applicable. The detailed integration framework, APIs, SDKs, and onboarding mechanisms for third-party media services and applications will be shared/provided based on the specific solution and integration requirements during the implementation/onboarding phase.
101	Media		Since Meghdoot is based on OpenStack, Kubernetes, and BOSS Linux, could C-DAC clarify the preferred deployment model for media workloads and whether solutions are expected to run on virtual machines, containers, Kubernetes clusters, bare-metal infrastructure, or a hybrid combination?	There is no single predefined deployment model. Depending on the workload and client requirements, media solutions may be deployed on virtual machines, containers/Kubernetes, bare-metal infrastructure, or a hybrid combination. The appropriate deployment model will be determined based on workload characteristics, performance requirements, and the target deployment environment.
102	Media		Could C-DAC provide clarity on the media storage architecture, including object, file, and block storage capabilities, expected performance characteristics, archival requirements, content lifecycle policies, and associated data protection needs?	Storage requirements will be project-specific.
103	Media		For services such as Media Transcoding, Live Video Streaming, Media Packaging, and Video Transport, could C-DAC specify the expected media formats, codecs, resolutions, streaming protocols, latency requirements, and throughput expectations that vendors should design for?	Media specifications will be project-specific.
104	Media		Can C-DAC confirm whether support for broadcast-grade workflows, including standards such as MXF, IMF, SCTE, SRT, RIST, HLS, MPEG-DASH, and low-latency streaming technologies, is expected as part of the Media Services roadmap?	Broadcast requirements will be project-specific.
105	Media		Would C-DAC clarify whether a Content Delivery Network (CDN) capability already exists within the Meghdoot ecosystem or whether vendors are expected to provide content distribution, caching, and edge delivery functionalities as part of their proposed solution?	No.depends on the Project requirement

106	Media		Does C-DAC envision Media Asset Management (MAM), Digital Asset Management (DAM), content cataloging, metadata management, workflow orchestration, and media supply chain automation capabilities as part of the proposed Media Services ecosystem?	MAM/DAM scope will be project-specific.
107	Media		Given that AI/ML Services are also included within the scope of the EOI, could C-DAC clarify whether AI-driven media capabilities such as automated metadata extraction, speech-to-text transcription, multilingual subtitling, content moderation, video indexing, and intelligent search are considered priority use cases?	Applicants may propose AI/ML capabilities such as metadata extraction, transcription, subtitling, content moderation, indexing, and intelligent search, where relevant to the proposed service and Meghdoot Cloud ecosystem.
108	Media		For service categories under the Media domain, will evaluation and empanelment be conducted independently for each service area, such as transcoding, streaming, storage, packaging, and ad insertion, or will preference be given to vendors offering a comprehensive end-to-end media platform?	Evaluation and empanelment shall be considered at the individual Cloud Service level, as applicable. Applicants may propose one or more Media Services based on their capabilities; offering an end-to-end platform shall not, by itself, be a mandatory requirement for empanelment.
109	Media		Can C-DAC clarify the technical acceptance criteria, performance benchmarks, scalability expectations, and certification processes that will determine successful integration and deployment of Media Services into the Meghdoot platform?	The detailed technical acceptance criteria, performance requirements, scalability parameters, and validation procedures shall be defined based on the specific Media Service and project requirements. The proposed service shall demonstrate successful integration and functional performance with the Meghdoot Cloud Suite.
110	Media		Can C-DAC share its vision for building a sovereign, India-owned Media Cloud platform comparable to global cloud media ecosystems and identify the highest-priority use cases across OTT streaming, broadcast transformation, sports media, digital archives, media asset management, AI-powered content operations, and next-generation content supply chains?	Applicants may propose relevant sovereign Media Services across OTT, broadcasting, digital archives, media asset management, AI-enabled content operations, and other applicable use cases, subject to the scope and objectives of the EOI.
111	Game Tech		Could C-DAC elaborate on its long-term vision for establishing a Sovereign Gaming Cloud ecosystem and identify the priority use cases, customer segments, and expected outcomes for the Game Tech category?	CDAC does not prescribe a specific long-term roadmap, customer segment, or outcome for the Game Tech category. Applicants may propose relevant Game Tech cloud services based on their existing capabilities and their applicability to the Meghdoot Cloud ecosystem.
112	Game Tech		Can C-DAC clarify whether the scope is limited to game server hosting infrastructure or includes a complete gaming backend platform consisting of matchmaking, session orchestration, player management, analytics, and live operations services?	The scope is not restricted to game server hosting infrastructure. Applicants may propose relevant gaming backend capabilities, including matchmaking, session management, player management, analytics, and live-operations services, where applicable to the proposed cloud service.
113	Game Tech		Could C-DAC provide expected scale expectations, including player concurrency, latency requirements, geographic coverage, and autoscaling requirements, to assist vendors in designing appropriate architectures?	CDAC does not prescribe fixed player concurrency, latency, geographic coverage, or autoscaling parameters at this stage. Such performance and scalability requirements shall be determined based on the specific service and project requirements.
114	Game Tech		Does C-DAC envision convergence between Game Tech and Media Services to support esports streaming, interactive live events, and gaming content distribution on the Meghdoot platform?	Integration between Game Tech and Media Services may be considered where relevant to the proposed solutions and project requirements. Such cross-category integration shall be evaluated based on technical feasibility and applicability to the Meghdoot Cloud ecosystem.

115	Game Tech		Would C-DAC be interested in AI-powered gaming capabilities such as player analytics, anti-cheat systems, intelligent NPCs, content moderation, recommendation engines, and Generative AI-driven game development accelerators as part of the sovereign gaming ecosystem vision?	AI-powered gaming capabilities may be proposed where relevant to the Game Tech service and the objectives of the EOI. The applicability of such capabilities, including analytics, anti-cheat, intelligent content, moderation, recommendations, and Generative AI, shall be evaluated based on the proposed solution and project requirements.
	Intimation to the Bidders			
	The Bidder must fill and submit the enclosed Annexure - K			
Corrigendum 3				
Sl. No	**EoI Section & Clause No**	**Page**	**Existing EoI Clause**	**Amended Clause**
1	Section II, Clause 2(iii) – Industries, Sl. No. 6 (Financial Stability)	Page 13	"Financial Stability – Certificate by statutory auditor to be submitted" (no threshold specified)	To encourage wider participation, it is proposed that the bidder be required to submit a Positive Net Worth Certificate covering the preceding three financial years, duly certified by its statutory auditor.

Annexure K

S.No	Category	Cloud Service Name