Sr No	**A. Cloud Infrastructure**	**Indicate Yes/No**
1	Biidders ability to provide **managed private cloud** services. The primary data Centre should be owned / managed & opreated by the bidder/ consortum partner by themselves to through third party (with full responsibility vesting with the bidder).	
2	Data-center shall be Tier III - TIA 942 compliant.	
3	Data-center well equipped with intrusion detection & protection systems, firewalls, system management solutions & tools, back-up & restore solutions, monitoring tools, network load balancer for applicable servers and network layer security to isolate the MUDRA production & test environment from other customers.	
4	The data-center's ability to scale up or down the servers/compute resources on-demad/ as desired without significant technical down time.	
5	The IT infrastructure should be hosted on private cloud. The cloud should have following capabilities:	
a	All the virtual machines should be auto scalable in terms of RAM and CPU.	
b	The cloud platform should ensure high availability across virtual machines.	
c	Cloud platform to support horizontal load balancing along with vertical load balancer to balance network traffic.	
d	Cloud provider should provide dashboard of all virtual machines to monitor resources allocated and used by the applications deployed.	
e	Cloud dashboard should permit generation of reports for trend analysis of system usage.	
f	There should be provision to generate historical reports of resources utilization.	
g	There should be admin panel to create, delete, start, stop, and copy virtual machines.	
h	There should be provision to take snapshots of machines so that working images of machines can be taken.	
	B. Disaster Recovery Management	
1	The DR site should be owned / managed & opreated by the bidder/ consortum partnerby themselves to through third party (with full responsibility vesting with the bidder)	
2	Disaster Recovery Services to ensure continuity of operations in the event of failure of primary data centre to meet the RPO and RTO requirements as specified by MUDRA.	
3	RPO should be less than or equal to 30 minutes and RTO shall be less than or equal to 4 hours	
4	During the change from Primary DC to DR or vice-versa (regular during drill or restoration after disaster), there should not be any data loss.	
5	There shall be asynchronous replication of data between Primary DC and DR and the Cloud Service Provider will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.	
6	Normally Primary Data Center will be the active server. The Disaster Recovery Site will remain on standby with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.	
7	In the event of a site failover or switchover, DR site will take over the active role, and all requests should be routed through DR site.	
8	During failover from primary DC to secondary (DR), compute environment for the application at DR site shall be **equivalent to DC** including all the security features and components of DC, without the failover components.	
9	The installed application instance and the database shall be usable and the same level of uptime of 99.5% as stipulated for DC shall be provided, when DR is activated.	
10	The bandwidth at the DR shall be scaled up to the level of Data center when DR is activated and other times it shall be adequate only to ensure replication of DC at DR.	

11	The service provider shall conduct live DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (regular planned changes), there should not be any data loss. The pre-requisite of DR drill should be carried out by service provider and MUDRA jointly. Certificate for DR drill should be submitted to MUDRA for compliance.	
12	The service provider shall clearly define the procedure for announcing DR based on the proposed DR solution. The service provider shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The service provider shall plan all the activities to be carried out during the Disaster Drill in consultation with MUDRA.	
13	The disaster recovery plan needs to be provided by the service provider which needs to be updated half-yearly.	
14	On successful award of the cobtract, the bidder will submit BCP plan to MUDRA.	
	C. Cloud Service Provisioning Requirements	
1	The Service provider should offer cloud service provisioning portal for MUDRA in order to provision cloud services either via portal, mobile app or automated using API.	
2	Cloud service provider should enable MUDRA to provision / change cloud resources through self service provisioning portal.	
3	The user admin portal should be accessible via secure method using SSL certificate.	
4	MUDRA should be able to set threshold of cloud resources of all types of scalability.	
5	MUDRA should be able to provision all additional storages required for cloud services.	
6	MUDRA should be able to predict his billing of resources before provisioning any cloud resources.	
7	MUDRA should be able to get list of all cloud resources from provisioning portal.	
8	MUDRA should be able to set the scaling parameters.	
9	MUDRA should be able to set percentage / quantity of RAM consumption to trigger new virtual machines.	
10	MUDRA should be able set percentage / quantity of CPU consumption to trigger new virtual machines.	
11	MUDRA should be able to set percentage / quantity of network bandwidth to trigger new virtual infrastructure.	
	D. Data Management	
1	Service provider should always ensure that data is destroyed whenever any cloud virtual machine is recycled or deleted.	
2	Service provider should clearly define policies to handle data in transit and at rest.	
3	Service provider should not delete any data at the end of contract period without consent from MUDRA.	
4	In case of scalability like horizontal scalability, the service provider should ensure that additional generated data is modified/deleted with proper consent from MUDRA.	
5	Service provider should ensure secure data transfer between Primary Data Center and Disaster Recovery site.	
6	Service provider should ensure data leakage protection and prevention.	
	E. Operational Management	
1	Service provider should upgrade its hardware time to time keeping in tune with EOL of the hardware to recent configuration to deliver expected performance for MUDRA.	
2	Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools.	
3	Service provider should manage their cloud infrastructure as per standard ITIL framework in order to deliver appropriate services to MUDRA.	
4	Service provider should deliver cloud resources with system for real time detection of resource requirement and automatic adjustments.	
	F. Cloud Network Requirement	

1	Service provider must ensure that cloud virtual machine of MUDRA is tenanted in a separate network and virtual LAN.	
2	Service provider must ensure that cloud virtual machines are having private IP network assigned to cloud VM.	
3	Service provider must ensure that all the cloud VMs are in same network segment (VLAN) even if they are spread across multi data centers of Service provider.	
4	In case of scalability like horizontal scalability, the Service provider should ensure that additional requirement of network is provisioned automatically of same network segment.	
5	Service provider must ensure that there is console access to cloud VMs, if MUDRA requires to access it using IPSEC/SSL or any other type of VPN.	
6	Service provider should ensure that cloud VM network is IPV6 enabled and all public facing devices are able to receive and transmit IPV6 data in addition to IPV4.	
7	Service provider should have provision of dedicated virtual links for data replication between their multiple datacentre in order to provide secure data replication for DR services.	
8	Service provider should ensure use of appropriate load balancers for network request distribution across multiple cloud VMs.	
	G. Datacenter specifications	
1	The primary and DR Site data-centers must be in India. The primary data centre must be located at Mumbai/ Thane/ Navi Mumbai. No data should be transferred out side India by the hosting service provider.	
2	The primary and DR site datacentres should be located in different seismic zones and not on same fault lines.	
3	The data centre (both primary and DR) should be MEITY empanelled.	
4	Proper Data Leak Prevention policies and processes must be in place	
5	The datacentres should have adequate physical security in place.	
6	The data-centers should conform to at least Tier-3 standards (certified under TIA942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.	
7	Data Centres should allow the access to physical audit of the data centres by MUDRA or any other third party authorised by MUDRA.	
8	Data Centres have to be PCI/DSS compliant.	
	H. Cloud Storage Service Requirements	
1	Service provider should provide scalable, dynamic and redundant storage.	
2	Service provider should offer to auto allocate more storage as and when required based on storage utilization threshold and also offer to provision from self-provisioning portal to add more storage as and when required by MUDRA.	
	I. Application Hosting Security	
1	Applications deployed should maintain a secure Password policy	
2	Applications deployed should be secured by using Intrusion detection system (IDS) and Intrusion prevention system (IPS) at network level.	
3	Have current vulnerability assessments and PCI (Payment Card Industry) scanning performed for all the applications hosted on the cloud.	
4	The Applications deployed should be secured through a Web Application Firewall (WAF) as a service.	
5	Bidder will have sole responsibility for fool-proof security of the applications and needs to provision all tools / real time monitoring to ensure the security of the application.	
6	Applications / Software Solutions shall comply with ISO 27001 Information Security Standard	
7	Applications / Software Solutions and infrastructure shall have Authentication – Authorization – Access audit trails	
8	Applications / Software Solutions shall be protected from security breaches, vulnerabilities	
9	All Service end-points- exposed over internet or internal shall be secured with at least 128 bits (desired 256 bits) SSL Certificates	
10	All Servers, Services, Applications / Software Solutions shall have hardened security and reviewed regularly.	
11	Any unauthorized access / attempt shall be reported immediately	

12	The entire data-center network shall have multiple levels of physical, logical, and network security systems for information protection including but not limited to IPSEC Policies, Firewalls, IDS / IPS protection Systems.	
13	Data center and its security should be compliant with RBI guidelines issued from time to time.	
14	The bidder should ensure application penetration testing once in a year and reports to be shared with MUDRA	
	J. Cloud Hosting Security	
1	Service provider should ensure there is multi-tenant environment and cloud virtual resources of MUDRA are logically separated from others.	
2	Service provider should ensure that any OS provisioned as part of cloud virtual machine should be patched with latest security patch.	
3	Service provider should implement industry standard storage strategies and controls for securing data in the Storage Area Network so that users are restricted to their allocated storage	
4	webService provider should deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.	
5	Service provider should have built-in user-level controls and administrator logs for transparency and audit control.	
6	Service provider cloud platform should be protected by fully-managed Intrusion detection system using signature, protocol, and anomaly based inspection thus providing network intrusion detection monitoring.	
7	Service provider would be responsible for proactive monitoring and blocking against cyber-attacks and restoration of services in case of attacks.	
	K. Cloud resource and Network monitoring	
1	Service provider should give provision to monitor the network traffic of cloud virtual machine.	
2	Service provider should offer provision to analyze of amount of data transferred of each cloud virtual machine.	
3	Service provider should provide network information of cloud virtual resources.	
4	Service provider should offer provision to monitor latency to cloud virtual devices from its data center or MUDRA should be able to set monitoring of latency to cloud VMs from outside world.	
5	Service provider must offer provision to monitor network uptime of each cloud virtual machine.	
6	Service provider must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.	
7	Service provider must make provision of resource utilization graph i.e. RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.	
8	Service provider must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.	
9	Service provider should give provision to monitor the uptime of cloud resources. The report should be in exportable form.	
11	Service provider should make provision to monitor the running process of Linux/Windows servers. This will help MUDRA to take the snapshot of processes consuming resources.	
12	Service provider must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.	
13	Service provider must ensure that audit logs of scalability i.e. horizontal and vertical is maintained so that billing disputes can be addressed.	
14	Service provider must ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.	
15	Service provider must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.	
16	Service provider should provide network information of cloud virtual resources.	
17	Service provider should offer provision to monitor latency to cloud virtual devices from its datacenter or MUDRA should be able to set monitoring of latency to cloud VMs from outside world.	
18	Service provider must offer provision to monitor network uptime of each cloud virtual machine.	

19	Service provider must provide utilization reports for Internet bandwidth, load balancers etc.	
	L. Application Performance Monitoring (APM)	
	a. Database monitoring:	
1	APM should be able to provide Overview of database server like Database details, version etc.	
2	APM should be able to provide host details which are connected to database Server	
3	APM should be able to provide session details of all active database sessions.	
4	Monitoring & management of network link proposed as part of this solution.	
5	APM should be able to provide server configuration details.(All configurations, advanced Configurations, Memory Configurations) Bandwidth utilization, latency, packet loss etc.	
	M. Backup Services	
1	Service provider must provide backup of cloud resources. Backups should be maintained at both off-site and on-site locations in secure fire proof and environmentally controlled environments so that the backup media are not harmed.	
2	Service provider should perform backup and restore management in coordination with MUDRA's policy & procedures for backup and restore, including performance of daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.	
3	Backup and restoration of Operating System, application, databases and file system etc. in accordance with defined process / procedure / policy.	
4	Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies	
5	Ensuring prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.	
6	Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.	
7	Media management including, but not limited to, tagging, cross-referencing, storing (both on-site and off-site), logging, testing, and vaulting in fire proof cabinets if applicable.	
8	Generating and sharing backup reports periodically	
9	Coordinating to retrieve off-site media in the event of any disaster recovery	
10	Periodic Restoration Testing of the Backup	
11	Maintenance log of backup/ restoration	
	N. Database Support Service	
1	Installation, configuration, maintenance of the database (Cluster & Standalone).	
2	Regular health checkup of databases.	
3	Regular monitoring of CPU & Memory utilization of database server, Alert log monitoring & configuration of the alerts for errors.	
4	Space monitoring for database table space, Index fragmentation monitoring and rebuilding.	
5	Performance tuning of Databases.	
6	Partition creation & management of database objects, Archiving of database objects on need basis.	
7	Patching, upgrade & backup activity and restoring the database backup as per defined interval.	
8	Schedule/review the various backup and alert jobs.	
9	Configuration, installation and maintenance of Automatic Storage Management (ASM), capacity planning/sizing estimation of the Database setup have to be taken care by the Bidder.	
10	Setup, maintain and monitor the 'Database replication' / Physical standby and Asses IT infrastructure up-gradation on need basis pertaining to databases.	
11	Tuning of high cost SQLs and possible solution to application development team for tuning in order to achieve optimum database performance.	
	O. Managed Services	
1	Network and Security Management: Monitoring & management of network link proposed as part of this solution.	

a	Bandwidth utilization, latency, packet loss etc.	
b	Call logging and co-ordination with vendors for restoration of links, if need arises.	
c	Redesigning of network architecture as and when required by MUDRA	
d	Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion protection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules. vi) Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately	
e	Ensure a well-designed access management process, ensuring security of physical and digital assets, data and network security, backup and recovery etc.	
f	Adding/ Changing network address translation rules of existing security policies on the firewall	
g	Diagnosis and resolving problems related to firewall, IDS /IPS.	
h	Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise MUDRA about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc	
2	Server Administration and Management:	
a	Administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and administrative support for print, file, and directory services.	
b	Setting up and configuring servers and applications as per configuration documents/ guidelines provided by MUDRA	
c	Installation/ re-installation of the server operating systems and operating system utilities	
d	OS Administration including troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required/ necessary for Windows, Linux or any other OS proposed as part of this solution whether mentioned in the RFP or any new deployment in future.	
e	Ensure proper configuration of server parameters, operating systems administration, hardening and tuning	
f	Regular backup of servers as per the backup & restoration policies stated by MUDRA from time to time	
g	Managing uptime of servers as per SLAs.	
h	Preparation/ updation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening	
	P. Helpdesk Support from Cloud Service Provider	
1	Service provider should provide flexibility of logging incident.	
2	The interface console of the incident tracking system would allow viewing, updating and closing of incident tickets	
3	Allow categorization on the type of incident being logged	
4	Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels	
5	Provide audit logs and reports to track the updating of each incident ticket	
6	It should be able to log and escalate user based requests.	
7	Service provider should allow ticket logging by email, chat or telephone.	
	Q. Hosting Infrastructure Technical Requirements	
1	Information Access / Transfer Protocol - HTTPS, REST over HTTPS	
2	Encryption - Minimum 128 bits, desired 256 bits, SHA2 support	
3	Interoperability - SOA, Web Services, Open Standard	
4	Scanned Documents - TIFF/ JPEG and/ or PDF for storage	
5	Document Encryption -PKCS Specifications	
6	Information Security - ISO 27001	
7	Operational Integrity and Security Management - ISO 27001	
8	Web / Portal Content - WCAG Level II compliant	
9	Service Management - ITIL v3 / ISO 20000	
10	Project Documentation - IEEE specifications for documentation	
11	Internet Protocol - IPv4 and IPv6 Compliant	
12	Device Supportability - Desktops/Laptops, Tablets (future provision for phone should also exist)	
13	Web Browsers - Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari	

14	Mobile Browsers - Microsoft Internet Explorer, Google Chrome, Android Web Browser, Apple Safari (iPhone/iPad), Mozilla Firefox All Web Browser backward compatible up to n-2 or HTML5 support	
15	Web standards - HTML5 Compliant, CSS, Java Script, JQuery / JQueryUI, Responsive Web	
16	Web Services - XML, REST, ODATA	
17	Database & Data Access -Oracle Database with ability to access ADO/ODBC / JDBC, ODATA	
18	Accessibility - As per Government of India Government of India, Section 280 for Accessibility Compliance	
19	Web Usability - As per Government of India Website/application design Guidelines, Bilingual Support (English/Hindi) for user input forms titles.	
20	Up time - Application uptime - 99.50% Data Center Availability– 99.8%	
21	Email System - SMTP, IMAP, POP3, Push Email, Directory Services Integrated	
22	Security, Penetration and Vulnerability Testing - A detailed test reports covering protection levels and vulnerable areas, and mitigation plan	
23	Application related - The protocols and middleware as per the delivered application should be supported seamlessly	