Department of Registration & Stamps, &

Department of Land Records

Maharashtra State,

Pune

Request for Proposal

Appointment of Cloud Service Provider to Migrate, Setup and Manage Primary (DC) & Disaster Recovery (NDR & DR) Site on Cloud

Table of Contents

Scope of Work

Department is currently hosting its applications with a DIT & MeitY empanelled Cloud service provider (ESDS) and all the applications are running on Government Community Cloud. DC is located at Mahape, Navi Mumbai & DR is located at Nashik. In addition some of the applications are hosted in National Data Centre (NDC) Pune. All the field offices and others are accessing all the applications from Cloud. As per the new directives from DIT, it is now required to avail new Cloud services or renew existing Cloud services through GeM eMarket place. With these directives, department as per the GeM guidelines, would like to invite bids from eligible bidders to provide 'Government Community Cloud Hosting & Managed Services

The broad project scope includes having a single service provider to provide cloud hosting and managed services for Department of Registration & Stamps and Land records Department, MS. The departments intend to procure the 'Government Community Cloud Hosting & Managed Services' for the business applications of Department of Registration & Stamps and Land records Department, MS. The shortlisted service provider shall provide the 'Government Community Cloud Hosting & Complete Managed Services', 'migrate the complete work load from existing Cloud to newly selected service provider through this bidding process through GeM eMarket place' for the period of 03 years, Department of Registration & Stamps and Land records Department, MS reserves the right to extend the services for another 02 years.

The proposed solution shall be scalable, extensible, highly configurable, secure and very responsive and shall support integration and optimization including scale up and scale down of required services and solutions (existing legacy and acquired in future), designed for or used by the Department of Registration & Stamps and Land records Department, MS

The broader requirements are expressed in the below –

- Cloud Infrastructure for Application Hosting (DC and DR).
- Migration from existing Cloud & NDC to newly selected service provider.
- Cloud Managed Services
- Provision of SMS Services for Department applications

1. General Requirements

The department is looking forward for the delivery of the following broad areas of services under this project:

1.2 Design of cloud infrastructure

- Bidder/CSP shall set up and manage the entire cloud solution deployed for department by Provisioning and Managing Cloud based resources. Bidder/CSP should have Government Cloud Community (GCC) for hosting government client and Applications for customers/ citizen in public domain i.e. DMZ and database MZ zone.

- The Bidder/CSP should ensure that the DC &DR site location is within India and the one of the DC is located in Maharashtra. Department may, at any point of time, undertake audit of the provisioned cloud environment; Bidder/Bidder/CSP is required to facilitate such timely audits as decided by the department.
- Bidder/CSP shall adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels (cloud services) mentioned in the RFP and the application service levels. There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA) during any unanticipated spikes in the user load.
- Bidder/CSP shall provide a detailed solution document for setting up of the DC & DR. The same shall be approved by the department project in-charge.
- Subsequently, the Bidder/CSP shall provision the entire infrastructure (compute, storage, network, security, software, bandwidth etc.) required for setting up of the DC & DR site as per the approved solution document.
- Bidder/CSP shall carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services. The final decision on capacity addition will be taken in consultation with department.
- The Bidder/CSP shall ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- The department will not be responsible if the Bidder/CSP has not provisioned some components, subcomponents, assemblies, and sub-assemblies as part of bill of material in the bid. The Bidder/CSP will have to provision the same to meet the solution requirements at no additional cost and time implications to department.
- The Cloud services shall be available on pay as per usage model. The billing shall be done monthly/quarterly irrespective of Fixed, On- Demand or mixed model of the Cloud Service Provider.

1.3 Deployment of solution on Government Community Cloud (GCC)

- The GCC shall be hosted on a separate isolated cloud at the Bidder/CSP's Data Center from other community cloud.
- GCC shall only host Cloud services for Departments / Ministries / Agencies / Autonomous Institutions / Statutory Bodies / Offices under Government of India or

States or UTs or Local Governments or PSUs within India (herein after referred to as Government Departments).

- The space allocated for the GCC infrastructure should be clearly demarcated and identified as hosting Government Departments' projects. The demarcated and identified area shall not host any components other than those of Government Departments' projects.
- The infrastructure elements including physical server, physical storage (including backup storage) and network equipment in the GCC shall be dedicated only for the Government Departments. There shall be physical and logical separation (of space, servers, storage, network etc.) from the public and other cloud offerings of the Cloud Service Provider. However, these infrastructure elements can be shared (physically only) among the Government Departments within GCC only.
- The entire Network Path for each of the hosted department applications shall be logically separate from that of other government departments.
- The entire Network path shall be administered through a Firewall with secured VLAN zoning.
- Bidder/CSP shall administer the Firewall policy as per department's directions. The Bidder/CSP shall also enable department to administer the firewall policy remotely. Bidder/CSP shall also provide read-only access of the firewall configuration to authorized personnel of department.
- With respect to monitoring tools, if any agent has to be deployed on the VMs or otherwise, the monitoring tools may be shared provided there is logical segregation and controls built- in to ensure that the tools & deployed agents comply to the security policies and ONLY the events, performance threshold alerts and inventory data for the OS, DB, infrastructure and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send Government Department's application and/or user and/or transaction data.
- Security solutions such as UTM, WAF, Anti-Virus, HIPS, Anti-DDoS, Anti-APT etc. shall be deployed (as shared service) for securing department applications on GCC
- Bidder/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 department must be within Indian Data Centre only. Bidder/CSP shall ensure that department data resides within India only. All monitoring, provisioning, should be within India and 100% isolated from other regions outside India, if in case Bidder/CSP has Global presence.
- The DR Solution shall be on Active (DC) – Standby mode.

1.4 Infrastructure Analysis and Build

- Bidder/CSP shall provide complete hardware details at DC & DR site including following parameters
    - CPU Calculation
    - RAM Calculation
    - Disk Calculation
    - Network interface requirement
    - Network throughput requirement
    - Backup requirement
- Bidder/CSP shall provide direct leased-line connections between the department-DC site and department- DR, if required or secured access has to be provided to office users.
- Bidder/CSP shall size the bandwidth requirements for the same. It is to be noted that department mandates for connectivity through the established ISPs.
- Proposed Solution should be compatible with IPv6 and High-level architectural diagram showing different layers of solution like Internet / P2P Connectivity, Network, Security, Compute, Hardware, Storage & Backup layers.
- Proposed solution should have IP schema depicted at high level with NATing to secure the applications directly getting exposed to Internet. Bidder/CSP should propose to deploy different applications and database in different VLANs with restricting users to directly access database layer and storage layer.
- Bidder/CSP shall provide Backup solution with different features, like snapshots of VMs, RDBMS backup, incremental and full back up of all data, restoration of data in test environment or as and when required.

1.5 Dynamic Scaling of Resources

- The initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) shall be carried out based on the information provided in the RFP.
- Subsequently, the Bidder/CSP shall 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 (upto 200%) and performance requirements of the solution and meet the SLAs. There should not be any constraints on the services.
- There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA) during any unanticipated spikes in the user load.
- The scaling up / scaling down has to be carried out with prior approval by the department.

- The Bidder/CSP shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.
- For any changes to the underlying cloud infrastructure, software, etc. under the scope of the Bidder/CSP, department shall get alerts / notifications from the Bidder/CSP, both as advance alerts and post implementation alerts.

1.6 Ownership of Data / VMs/ Software

- Department shall retain ownership of all data & applications hosted on Bidder/CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time (without additional charges).
- Department retains ownership of all virtual machines templates, clones, and scripts/applications created for the department's application. Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time (without additional charges).
- Department retains ownership of loaded software installed on virtual machines and any application or product that is deployed by department on the Cloud Infrastructure.

1.7 Compliances

- Bidder/CSP shall adhere to the standards published (or to be published) by department or any standards body setup / recognized by Government of India and notified to the Bidder/CSP by department as a mandatory standard.
- The Bidder/CSP's cloud service offerings shall always remain Empaneled / complied with the MEITY guidelines & standards. Bidder/CSP shall be responsible for the costs associated with implementing, assessing, documenting and maintaining such Empanelment/Compliances.
- Bidder/CSP shall always remain adhered to the prevailing guidelines issued by NCIIPC, RBI, CERT-In etc. from time to time.

1.8 Documentation

- Bidder/CSP shall create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.
- The documents which hold critical information, process, policies shall have to be approved by department before release.
- The Bidder/CSP shall develop, maintain, update following documents as per department requirements:
    - Details of inventory for Compute, Storage, Network, Security elements.
    - Details of the management, monitoring and helpdesk tools

- The WAN connectivity plan
- Business Continuity/DR plan
- Details of manpower deployment at NOC and SOC
- Escalation matrix.
- Other details as desired by department

1.9 Resource Management

- The Bidder/CSP shall manage the instances of storage, compute instances, and network environments. This includes department owned & installed operating systems and other system software that are outside of the authorization boundary of the Bidder/CSP.
- The Bidder/CSP shall enable workflow based automatic switch over/ failover between DC & DR.
- The Bidder/CSP shall provide a webpage and associated Uniform Resource Locator (URL) that describes the following:
  - Service Level Agreements (SLAs)
  - Help Desk and Technical Support
  - Resources (Documentation, Articles/Tutorials, etc.)

1.10 Operation Services

- Bidder/CSP shall ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
- Bidder/CSP shall manage the network, storage, server, and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs.
- Bidder/CSP shall ensure monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access within the Bidder/CSP's boundary.
- Prepare a comprehensive O&M plan for managing the cloud services and keep it updated.
- Bidder/CSP shall ensure uptime and utilization of the cloud resources as per SLAs defined in this RFP.
- Bidder/CSP is required to provision additional VMs when the utilization exceeds 80%.
- Bidder/CSP shall manage the cloud infrastructure as per standard ITIL framework.
- Bidder/CSP shall investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools.
- Bidder/CSP shall design and implement automated scaling processes
- Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be supported by the Bidder/CSP for the entire contract period at no extra cost to department.
- Bidder/CSP shall provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- Bidder/CSP shall provide 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.

- Bidder/CSP shall document and perform patch management appropriate to the scope of their control and/or Provide self-service tools to perform patch management. Generate Alerts well in advance on the upcoming patches via email and management portal.

1.11 Self Service Management /Provisioning

- Self Service management / provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.
- The Bidder/CSP shall provide Self Service Provisioning Portal / Basic monitoring tool / Dashboard with two factors authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.
- It shall enable department to provision virtual machines, storage, and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
- It shall enable service provisioning via online portal/interface (tools).
- It shall enable service provisioning via Application Programming Interface (API).
- It shall enable secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]
- It shall Support the terms of service requirement of terminating the service at any time (on-demand).
- It shall make the Management Reports described in this RFP accessible via online interface. These reports shall be available for one year after being created.
- The Bidder/CSP shall ensure that effective Remote Management features exist so that issues can be addressed by department in a timely and effective manner.
- The Bidder/CSP shall provide for automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
- The Utilization Monitoring tools shall have minimum following features:
    - Real time performance thresholds.
    - Real time performance health checks.
    - Real time performance monitoring & Alerts.
    - Historical Performance Monitoring.
    - Capacity Utilization statistics
    - Cloud Resource Usage including increase / decrease in resources used during auto-scale
- The Bidder/CSP shall provide Trouble Ticketing via online portal/ interface (tools).
- The Bidder/CSP shall support maintenance of user profiles and present the user with his/her profile at the time of login

1.12 Data Management

- The Bidder/CSP shall strictly manage data isolation in the multi-tenant environment.
- The Bidder/CSP should provide tools and mechanism to department (or its appointed agency) for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.

- Bidder/CSP shall facilitate Transfer of data back in-house, either on demand or on termination of contract for any reason.
- Bidder/CSP shall manage data reminisce throughout the data life cycle.
- Bidder/CSP shall provide and implement security mechanisms for handling data at rest and in transit.
- Bidder/CSP must not delete any data at the end of the agreement (as per Exit Management Clause) without the express approval of department.
- When Bidder/CSP (with prior approval of department) scales down the infrastructure services, Bidder/CSP is responsible for deleting or otherwise securing department's Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered

1.13 User Administration

- Bidder/CSP shall Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege principles and ensuring that users have only those permissions necessary to perform their assigned tasks.
- Bidder/CSP shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
- Bidder/CSP shall Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it for cloud portal.

1.14 Help Desk

- Bidder/CSP must provide multiple support options catering to the varying levels of support requirements (e.g., toll free number, ticket, chat and forum) for department.
- Department project manager shall be periodically visiting the data center site on quarterly basis or as and when required. Bidder/CSP shall make convenient & secure provisions for at least 2 department personnel to access the department cloud infra and meeting with stack holder who all are providing the support service to department.
- The Bidder/CSP must have Fire-proof space (with Lock & Key). If required Bidder/CSP allow to store department items, equipment etc. Fire proof space should be under 24 x 7 under CCTV monitoring.
- The Bidder/CSP should ensure availability of atleast one dedicated support person having 5+ years of experience in Managing services for Cloud Infrastructure in department premises during the entire duration of the project.

1.15 Cloud Resource and Network Monitoring

- Bidder/CSP shall provision to monitor the network traffic in department cloud landscape.
- Bidder/CSP shall provision to analyze amount of data transferred of each virtual machine.
- Bidder/CSP shall provide network information of cloud virtual resources.
- Bidder/CSP shall provision to monitor latency to cloud virtual devices from outside world.

- Bidder/CSP shall provision to monitor network uptime of each cloud virtual machine.
- Bidder/CSP shall provision for resource utilization i.e. CPU graphs of each virtual machine.
- Bidder/CSP shall provision for resource utilization graph i.e. RAM of each virtual machine.
- Bidder/CSP provision for resource utilization graph i.e. disk of each virtual machine. There shall be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.
- Bidder/CSP shall provision to monitor the uptime of cloud resources. The report shall be in exportable form.
- Bidder/CSP shall provision to monitor the load of Linux/Windows servers and set threshold for alerts.
- Bidder/CSP shall provision to monitor the running processes of Linux/Windows servers. This will help department to take the snapshot of processes consuming resources.
- Bidder/CSP shall provision for setting alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.
- Bidder/CSP shall ensure that there should be historical data of minimum 6 months for resource utilization to resolve any billing disputes if any.
- Bidder/CSP shall ensure that audit logs of scalability i.e. horizontal and vertical is maintained so that billing disputes can be addressed.
- Bidder/CSP shall ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.
- Bidder/CSP shall ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.
- Bidder/CSP shall provide utilization reports for Internet bandwidth, load balancers etc.
- Bidder/CSP shall provide ability monitor table space health and size.
- Bidder/CSP shall provide ability to display live and waiting session.
- Bidder/CSP shall provide ability to display live processes. Monitor pmon, smon, dbwr, lgwr, ckptr for monitoring availability of Oracle.
- Bidder/CSP shall provide ability of Monitoring & management of network link proposed as part of this solution.
- Bidder/CSP shall provide ability to display monitoring parameters for continuous monitoring bandwidth utilization, latency, packet loss etc.
- Bidder/CSP shall provide solution for Monitoring Parameters Buffer Cache Size, Shared Pool Size
- Bidder/CSP shall provide solution for Monitoring Parameters Redo Log Buffer Size, Fixed Area Size
- Bidder/CSP shall provide solution for Monitoring Parameters Java Pool size, Free Memory, Total free able PGA, Maximum PGA allocated, Total PGA allocated, Total PGA used, Cache Hit Percentage.

1.16 Cloud Compute Requirements

1.17 Provisioning of Virtual Machines (VM)

- The Bidder/CSP shall do provisioning for required computing resources for hosting of all the required IT applications as listed. All Application and DB servers shall be deployed on enterprise class Type-I hypervisor based Virtualized environments. Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc. The Bidder/CSP shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio.
- CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2.4GHz. The CPU shall support 64-bit operations.
- Department reserves the right to get the landscape audited by any third party auditor, if deemed necessary.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application.
- Provide facility to configure virtual machine of required vCPU, RAM and Disk.
- Provide facility to use different types of disk like SAS, SSD based on type of application

1.18 Administration, Configuration & Training

- Upon deployment of virtual machines, the Bidder/CSP has to assume full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required.
- Bidder/CSP shall ensure Preparation / Updation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.
- Bidder/CSP shall ensure Patching of VMs on the next available patch management change window and / or provide self-service tools to patch VMs.
- The Bidder/CSP shall be setting up and configuring servers and applications as per configuration documents/ guidelines provided by department.
- The Bidder/CSP shall do Installation/ re-installation of the server operating systems and operating system utilities in the VMs.
- Bidder/CSP shall make provision to Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
- Bidder/CSP shall monitor availability of the servers, Bidder/CSP-supplied operating system & system software, and Bidder/CSP's network.
- Bidder/CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.

- Bidder/CSP shall arrange training for department personnel on proposed cloud platform from OEM with certification.

1.19 Internal Storage Requirements of VMs

- The Bidder/CSP shall provide scalable, redundant, dynamic Web-based storage.
- The Bidder/CSP shall provide SSD based block storage capabilities on-demand, dynamically scalable per request for virtual machine instances of arbitrary size ranging from 1GB to TBs.
- The Bidder/CSP shall provide options to use different types of disks based on performance requirement of the hosted application stack. Once mounted, the block storage should appear to the virtual machine like any other disk.
- Bidder/CSP shall enable department to add either block storage volume or file level storage block to cloud VM from provisioning portal.
- There has to be different disk Space options to allocated for virtual machines and file data as per the requirement of department.

1.20 Network Interfaces & Segmentation of VMs

- Bidder/CSP shall ensure that cloud VM network is both IPV4 & IPV6 compatible.
- Bidder/CSP must ensure that cloud virtual machines are into separate network tenant and virtual LAN.
- Bidder/CSP shall provide Private static IP addresses for all the VMs.
- Bidder/CSP must ensure that all the cloud VMs are zoned in different network segments (VLANs) as per department requirements.
- Bidder/CSP shall ensure the VMs provisioned should have minimum 4 no's of 10G vNIC and should be scalable to 25G each.
- Bidder/CSP should ensure sub-millisecond latency between VMs within same data center.

1.21 Security of VMs

- VMs should be firewall protected
- VMs should have Host based Security Software.
- The Bidder/CSP shall provide Identity and Access Management for managing access to department users
- Hardening & patch management of underlying infrastructure by Bidder/CSP
- Management of the OS processes and log files of the VMs
- Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
- Management of the OS processes and log files including security logs retained in guest VMs.

1.22 Server Load Balancing

- Cloud service should deploy a Load Balancer to distribute the TCP, UDP, HTTP, HTTPs traffic across many computing resources within the same site to increase the responsiveness and availability of applications.

- Cloud service should provide secure, hardened, redundant (hardware or software) based Load balancer services

1.23 Backup/ Restoration / Migration / Deletion of VM Images and data

- Bidder/CSP shall provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing. It shall allow take an existing running instance (or a copy of an instance) and export the instance into a department's approved image format. Entire VM data backup must be available to department.
- Bidder/CSP shall have provision for automatic restart (HA) of virtual machine on another physical server in case of host server failure.
- Bidder/CSP shall have provision for live migration of virtual machine to another physical servers and vice versa in case of predictive server failure. Bidder/CSP shall perform an Image backup of department VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into User department(s) required format.
- In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time without having to reinstall or reconfigure the VM for the department solution.
- In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to department as per stipulations and shall ensure that the data cannot be forensically recovered.

1.24 Provisioning of Operating System & other Software

- Bidder/CSP shall provide adequate licenses for Operating system and other software (other than those in scope of department).
- Bidder/CSP shall be able to support major Linux distributions - (Oracle Linux, Red Hat, SUSE, Ubuntu, Centos, and Debian etc.)
- Bidder/CSP shall support latest Windows Server versions as per department requirements.
- Bidder/CSP shall offer license portability and support for Microsoft products etc.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions
- Software (limited to OS, security solutions and other platform stack where offered by the Bidder/CSP to department) will never be more than one versions behind unless deferred or rejected by department. This is not applicable to software such as cloud management stack

1.25 Provisioning of Database Servers and DBA Services

- Bidder/CSP shall do provisioning for required Database Servers and Database administrator services for operating IT applications.
- Bidder/CSP shall offer the Database service that makes it easy to set up, operate, and scale a relational database in the cloud.

- Cloud service should support latest version of all major database like MS SQL, My SQL, PostgreeSQL, MariaDB, DB2, Sybase, MaxDB, HANA etc...
- Cloud service should support asynchronous replication of the primary database to secondary database (and vice versa) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
- Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
- Cloud service should support a manual failover of the DB instance from primary to a standby replica.
- Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
- Cloud service should support creating multiple in-datacenter and across datacenter replicas within India per database instance for scalability or disaster recovery purposes.
- Cloud Service should support enhanced availability and durability for database instances for production workloads.
- Cloud service should support creating a DB back up and restoring the DB instance from the backup to a specific date and time.
- Cloud service should allow monitoring of performance and health of a database or a DB instance.
- Bidder/CSP shall perform following Database support services:
    - Installation, configuration, maintenance of the database (Cluster & Standalone).
    - Regular health check-up of databases.
    - Regular monitoring of CPU & Memory utilization of database server,
    - Alert log monitoring & configuration of the alerts for errors.
    - Space monitoring for database table space, Index fragmentation monitoring and rebuilding.
    - Performance tuning of Databases.
    - Partition creation & management of database objects, Archiving of database objects on need basis.
    - Patching, upgrade & backup activity and restoring the database backup as per defined interval.
    - Schedule/review the various backup and alert jobs.
    - Setup, maintain and monitor the 'Database replication' / Physical standby and Assess IT infrastructure up-gradation on need basis pertaining to databases

1.26 Storage Provisioning

- Bidder/CSP shall do provisioning for required Storage for hosting of IT applications.
- Bidder/CSP shall provide scalable, dynamic, and redundancy storage. Bidder/CSP shall offer Block / File Object level storage to use with compute instances in the cloud.

- Bidder/CSP shall have following storage offerings to address different kind of department's needs.
- The storage array should support hardware-based data replication at the array controller level across all models of the offered family.
- Bidder/CSP shall provide facility to use different types of disk like SAS, SSD based on type of application. Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
- Cloud service should support consistent low latency performance between 5-15 ms at any scale.
- The application and database storage shall be provided on high speed disks (minimum 3IOPS/GB) for better performance. Bidder/CSP shall deliver disks with minimum 5 IOPS per GB for OLTP load. The IOPS for NON OLTP load should be minimum 3 IOPS per GB.
- Bidder/CSP shall allow minimum block of 1 GB to be provisioned by department from self-service provisioning portal.
- Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
- Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).

1.27 Storage Service Management

- Bidder/CSP shall provide storage management tools to cater dynamically scalable storage requirements of department.
- Bidder/CSP shall facilitate following storage services:
  - Storage Administration
  - LUN management-LUN provisioning and deletion, LUN mapping to the host
  - RAID group creation
  - SAN Switch management, SAN switch configurations (zoning, masking)
  - Controller configuration
  - License management
  - Firmware upgradation

1.28 LAN Networking Requirements

- Bidder/CSP shall provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from Bidder/CSP pool.
- Local Area Network (LAN) shall not impede data transmission.
- Bidder/CSP shall deploy VMs in separate security zones / network isolation layers.
- Provide private LAN connectivity between primary DC and DR facilities.
- IP Addressing:
  - Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).

  - Provide IP address and IP port assignment on external network interfaces.
  - Provide dedicated virtual private network (VPN) connectivity.
- The NOC / SOC facility shall be physically located at the site of proposed DC and should not be remotely managed.

1.29 IT Network Management Services

- The Bidder/CSP shall perform Monitoring & Management of network links proposed as part of this solution.
- The Bidder/CSP shall provide tools to monitor Bandwidth utilization, latency, packet loss etc.
- The Bidder/CSP shall provide support in Call logging and co-ordination with vendors for restoration of links if need arises.
- The Bidder/CSP shall provide support for Redesigning of network architecture as and when required by department.
- Bidder/CSP shall give provision to monitor the network traffic of cloud virtual machine.
- Bidder/CSP shall offer provision to analyze of amount of data transferred of each cloud virtual machine.
- Bidder/CSP shall provide network information of cloud virtual resources.
- Bidder/CSP shall offer provision to monitor latency to cloud virtual devices from its datacenter or from outside world.
- Bidder/CSP must offer provision to monitor network uptime of each cloud virtual machine

1.30 Maintenance & Support of implemented Cloud

- The Bidder/CSP shall be responsible for providing 24*7*365 days' support to the infrastructure for from the date of issuance of operational acceptance by department. Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of Bidder/CSP.
- The Bidder/CSP shall conduct vulnerability and penetration test (from a third-party testing agency which may be CERT-IN empaneled) on the Cloud facility every 6 months and reports should be shared with department. The Bidder/CSP needs to update the system in response to any adverse findings in the report, without any additional cost to department.
- Bidder/CSP is required to provision additional VMs when the utilization exceeds 80%.
- The Bidder/CSP shall develop appropriate policy, checklists in line with ISO 22301, ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site.
- On expiration / termination of the contract, Bidder/CSP shall handover complete data in the desired format to department which can be easily accessible and retrievable

1.31 Hardware Upgrades/ Software Updates / Patch Management

- Bidder/CSP shall perform patch management appropriate to the scope of their control and/or provide self-service tools to perform patch management. Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be done by the Bidder/CSP for the entire contract period.
- Application Patch Updation will be done by department team.
- Bidder/CSP shall Document all patch management related activities within the Bidder/CSP's scope.
- The Bidder/CSP shall ensure to Generate Alerts well in advance on the upcoming patches via email and management portal.

1.32 Self Service Provisioning Portal

- The solution should have ability to automatically provision services via a Web Portal (Self Provisioning), provide meter billing, to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota, and show-back information is essential for the private cloud platform to be offered.
- The Self-Service Provisioning Portal / Basic monitoring tool / Dashboard should have two factor authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.
- The Bidder/CSP support team shall Interface with the technical team of Bidder/CSP on behalf of department for all activities including monitoring the reports (e.g., usage, security, SLA,), raising (or escalating) tickets / incidents and tracking the same to resolution.

1.33 Data Handling

- The Bidder/CSP shall strictly maintain isolation of department's data isolated from other client in multi-tenant environment. Provide and implement security mechanisms for handling data at rest and in transit.
- In order to maintain confidentiality of department's data, Bidder/CSP shall further ensure with an undertaking that the data cannot be forensically recovered after its deletion. The Bidder/CSP should provide tools and mechanism to department or its appointed agency for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.
- The Bidder/CSP shall manage data reminisce throughout the data life cycle. Bidder/CSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of department.
- The Bidder/CSP shall provide mechanism to transfer data back in-house either on demand or in case of contract or order termination for any reason. On expiration/ termination of the contract, Bidder/CSP shall handover complete data in the desired format to department which can be easily accessible and retrievable.

1.34 Monitoring Tools for Bidder/CSP Services

- Bidder/CSP shall provide monitoring solution for real-time monitoring of Network, IPs, subnet, Servers, Storage, Uptime, Service status, and should be capable of reporting SLA violations.
- OEM support for the monitoring solution proposed should be available throughout the contract period with access to software updates, maintenance patches and version upgrades.
- Bidder/CSP shall provide solution to help department monitor RPO of each application in near real-time and RTO during DR drills.
- Provision tool should allow to configure the workflow of switchover/switchback

1.35 Reports & Documentation

1.36 MIS Reports

- Bidder/CSP shall submit the reports on a regular basis in standard format. The following is only an indicative list of MIS reports that may be submitted;

Sr No	Report Type	Frequency
1	• Summary of resolved, unresolved and escalated issues / complaints • Log of backup and restoration undertaken	Daily
2	• Summary of systems rebooted. • Summary of issues / complaints logged with the OEMs. • Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc. • Hypervisor patch update status of all servers where department Virtual Machines running.	Weekly
3	• Availability reports of Servers / Virtual machines • Consolidated SLA / Non-conformance reports	Monthly

	• Summary of component wise uptime • Log of preventive / scheduled maintenance undertaken • Log of break-fix maintenance undertaken • All relevant reports required for calculation of SLAs	

▪	• Consolidated component-wise availability and resource utilization
	• All relevant reports required for calculation of SLAs and verification of Invoices.
	• Logs and Audit Trails
	  ○ Log Access Availability (what log file entries department has access to).
	  ○ Logs retention period (the period during which logs are available for analysis).
	  ○ Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.
		Quarterly

1.37 Alerts & Notification

- Bidder/CSP shall offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
- Bidder/CSP shall offer a cost-effective outbound-only email sending service.
- The Bidder/CSP shall provide the infrastructure performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
- Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
- Notifications should be triggered each time a configuration is changed

1.38 Usage Reporting and Billing Management

- Track system usage and usage reports.
- Monitoring, managing, and administering the monetary terms of SLAs and other billing related aspects.
- 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 (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.

1.39 Escalation Matrix & Team Member details

- The Bidder/CSP shall provide updated escalation matrix either by email, at least once in a quarter or whenever there is a change in the escalation matrix whichever is earlier.
- The Bidder/CSP shall also provide team member details for following teams:
  - Support Team
  - DR Drill Team

1.40 Disaster Recovery Services

1.41 Overview

- Bidder/CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center. Bidder/CSP shall design and document an efficient disaster recovery solution in lines with the requirements of department and as per the RPO and RTO requirements.
- The solution should be architected to run on cloud services to provide business continuity with no interruptions in case of any disruptions /disaster at DC through semi-automated processes of redirecting the department data traffic to DR site.
- During normal operations, the Primary Data Centre will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available as per the solution offered.
- The application environment shall be installed and ready for use.
- The Bidder/CSP should offer switchover and switchback of individual Servers / VMs/Applications /Components instead of entire system.
- Till a disaster (planned/ testing or otherwise) is declared by department the users should not be allowed to access the IT applications from DR site (or as per discretion of department).

1.42 RPO & RTO Requirements

- The service parameters to be met by the DR system focus on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), which in business terms define the 'Interruption to Service' and 'Loss of Data' respectively. The RTO will be calculated from the time of “declaration of a disaster” up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations.

- The Recovery Time Objective (RTO) shall be less than or equal to 60 minutes to enable business operations & The Recovery Point Objective (RPO) should be Near Zero
- The Bidder/CSP should offer dashboard to monitor RPO and RTO

1.43 Replication Requirements

- Bidder/CSP shall adequately do the sizing of DC-DR replication links and commission them with (1+1) redundancy, to meet the RTO and the RPO requirements.
- DR Transactional Databases 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 Centre (PDC) site. There shall be asynchronous replication of data between Primary DC and DR. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to department.
- Bidder/CSP shall be responsible for providing/facilitating replication tools / software/ processes for Databases, Active Directory, Web Servers, application etc. for seamless replication from DC to DR and vice versa to meet RPO and RTO requirements.
- Bidder/CSP shall provide detailed operating manuals for replicating these solutions.
- The Bidder/CSP shall deploy these tools after acquiring consent from department's project incharge.
- The Bidder/CSP shall provide details of replication mechanism for (but not limited to) the following solutions:
    - Operating system
    - Database
    - Application server
    - File server
    - Email server
    - Active Directory/LDAP

1.44 DC-DR Failover & Restoration - Mock Drills / Actual Disaster

- The Bidder/CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR.
- The failover from primary DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, the system at proposed Bidder/CSP's DR Data Center will be primary system.
- The DR should be available (with its data) on-demand basis within the defined RTOs and RPOs, wherein 100% of the services of DC would run from DR site. All users of department will connect to Bidder/CSP's system through Internet link.
- During the drill, the Bidder/CSP shall demonstrate the fulfilment of SLAs at load of 100% users with 60% concurrency.

- The use of Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.
- Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The installed application instance and the database shall be usable.
- During the change from DC to DRC or vice-versa (regular planned changes), it should be as per the given RPO. Bidder/CSP shall provide work flow based switchover/ failover facilities (during DC failure & DR Drills). The switchback mechanism shall also be work flow based. The Bidder/CSP shall also provide a tool/ mechanism for Department to trigger DR switchover, for example a "one-click DR". Bidder/CSP shall provide support for the development and configuration of any additional scripts for successful working of DR.
- The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site.
- Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.
- Bidder/CSP shall provide detailed DR activity plans which will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site.
- Bidder/CSP shall also document steps for restoring services from DR site to DC site.
- In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.
- The Bidder/CSP shall conduct DR drill at the interval of not more than six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. The pre-requisite of DR drill should be carried out by Bidder/CSP and department jointly. The exact process of the DR drill should be formulated in consultation with the department team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the Bidder/CSP as part of the disaster recovery plan. Bidder/CSP shall plan the activities to be carried out during the mock drill and issue a notice to the department at least 15 working days before such drill.
- During the DR drill, the Bidder/CSP need to arrange the full DR team with sufficient resources and expertise and complete the activity under

the supervision of senior resource for co-ordination. The Bidder/CSP shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site.

1.45 DR Services

- Provision for managed services for the entire DR facility will be required. Bidder/CSP shall provide continuous maintenance activities to support the disaster recovery site. This includes (but not restricted to):
- Bidder/CSP shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, repairs, part replacement etc. from certified vendors. ITIL processes named problem, change, incident & configuration will be followed by Bidder/CSP at DR site.
- Bidder/CSP should have proper escalation procedure and emergency response in case of failure/disaster at DC.
- Bidder/CSP may partner with respective application / product support vendor to support DR in event of disaster or for performing periodic maintenance & upgrade activities
- Bidder/CSP shall perform RPO monitoring, reporting and event analytics and other activity associated with operations and management of DR plan and Implementation for the disaster recovery solutions.
- Bidder/CSP shall provide a monitoring tool with dashboard showing RPO, RTO, changeover facility etc.
- The date, time, duration, and scope of each drill shall be decided mutually between department and the Bidder/CSP. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
- To demonstrate how the application fails over when the primary site goes down. The testing should include the:
    - Uninterrupted replication to DR servers.
    - Lag in replication due to any unforeseen errors.
    - Process of recovering from lags if any.
    - Data integrity test of DR servers.
- The Bidder/CSP shall be responsible providing input for
- Devising and documenting the DR policy discussed and approved by department.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.
- Bidder/CSP shall support in bringing the machines to login level in case of disaster / DR drills. Provisioning, configuring, and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router.
- The solution is envisaged for application level recovery scalable to site level recovery based on the impact of the disaster.

- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the Bidder/CSP.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.

1.46 Business Continuity Planning

- Bidder/CSP shall define and submit (as part of the solution), a detailed approach for "Business Continuity Planning"; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which "disaster" would be declared.
- The Bidder/CSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.
- The Bidder/CSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.
- Incident response plans should be developed by the Bidder/CSP which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

1.47 Backup & Restore Service

- Bidder/CSP shall provide backup solution (Disk / Tape based backups), covering but not limited to 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.
- Bidder/CSP shall cover (not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.
- Bidder/CSP shall Configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy/procedure/plan finalized by department.
- Bidder/CSP shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
- The disk-based backup solution must have the feature to integrate with any Tape Library.
- Bidder/CSP should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
- The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.

- The backup service should support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc.
- Department should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.
- Bidder/CSP shall restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month for data that can be restored from a local copy.
- Bidder/CSP shall Provide and install additional infrastructure capacity for backup and restore.
- There has to be provision if required to shift the backup at department required location on tape/USB.
- Bidder/CSP shall perform restoration testing biannually with the permission of department.
- Bidder/CSP must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
- Bidder/CSP shall ensure prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
- Bidder/CSP shall perform 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.
- The backup service must provide following capabilities.
  - Compression: Support compression of data at source before backup
  - Encryption: Support at least 128-bit encryption at source
  - Alert: Support email notification on backup job's success / failure
- File exclusion: Ability to exclude specific files, folders, or file extensions from backup
- Deduplication: Provide deduplication capabilities
- Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups.
- Indicative Backup plan

#	Backup Type	Backup Frequency	Retention Period
1	Incremental	Daily	7 Days
2	Full	Weekly	1 Month
3	Full	Monthly	12 Months
4	Full	Yearly	7 Years

#	Restoration Policy	
1	Backup taken in last month	Once in a Month
2	Backup taken in last quarter	Once in a Quarter

1.48 Migration Service

- Bidder/CSP should support end to end migration from existing environment (ESDS & NDC) to the new environment.

1.49 Pre-requisites

- Following tasks shall be carried out to determine the current inventory, assess the current environment to determine which workloads and applications are critical and because of which there may be a loss to department.
- Analysis to identify the IT users and stakeholders that would be impacted by cloud migration.
- Identify the business processes and governance processes that are associated with current inventory (both applications & infrastructure).
- Formulated a baseline of department's technical environment including inventory of both infrastructure and applications, to include development/testing environments.
- Bidder/CSP shall provide Application Management Services during migration period.
- Bidder/CSP would be required to understand the complete Application landscape so as to provide Application management.
- All the required support for application to ensure its smooth running, data consistency, performance will be responsibility of Bidder/CSP.
- Understanding of the implications of moving individual applications or groups of applications to the cloud.
- Decomposition of applications & identification of common functions and services that can potentially be migrated to the cloud, and identification of potential shared services. Comprehensive analysis and understanding of the current environment, that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery and analysis of which on premise technical resources / applications are best suited for the cloud

1.50 Migration Planning

- Comprehensive planning for migration of the application suite and data to the cloud including developing the migration roadmap identifying the constraints and inhibitors to cloud migration. The migration plan should detail out:
  - The configuration proposed to fulfil day-1 requirements with the explicit understanding that during the duration of the contract these nominal profile requirements will change
  - Migration Tools, software, applications, scripts, and associated licenses has to be planned and documented.
  - Procedures and documentation to be developed for migration of applications and data & content including redevelopment/additional development that may be required
  - Plans for co-existence of non-cloud and cloud architectures during and after migration
  - Communication, change management, and training needs

- Cloud governance for post-implementation
- Test Plans for verifying successful migration
- Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the Bidder/CSP will undertake to help avoid identified risks connected with the Migration.

1.51 Migration

- Changes to the applications based on:
  - Complete architectural understanding of the existing applications and processes necessary for successful migration of the applications and data as well as continued operation and maintenance of the services.
  - Analysis of the interdependencies such as application dependencies and affinities to servers, server configuration etc.
  - Dependencies between applications and data.
- Provision the necessary compute & storage infrastructure on the cloud including the underlying software licenses to host the Application Suite that meet or exceed the day-1 minimum capacity.
- Setup of Development, Quality, Production and Disaster Recovery Environments by provisioning the necessary compute & storage infrastructure on the cloud along with the underlying software licenses to host the Application Suite.
- Configuring external connections to the hosted infrastructure required to upload database backups and virtual machine (VM) images to the hosting environment.
- Migration of the Application Suite from the existing infrastructure to the cloud infrastructure. The migration (supported by SI) shall also include the migration of underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.
- To enable easy migration to cloud, department may consider up-gradation of OS & DB to latest version available in market.
- Deployment of the new Applications on the cloud environment as per the to be architecture.
- Configure, manage, deploy, and scale the system on environments setup on cloud

1.52 Managing and Monitoring of Migration

- Manage (including project managing), coordinating and planning all aspects of migration.
- Proactively identify, monitor, and manage any significant risks or issues in relation to migration.
- Provide regular progress reports to the department
- A listing of all Migration Deliverables and Milestones, including acceptance status, the estimated time to completion, days overdue, planned completion date, and actual completion date and comments, as well as a report identifying the status of all Milestones (for example: red, amber, green).

- A listing of all unresolved issues related to the execution of the Migration Plan, along with due dates, priority, responsible party, and an assessment of the potential and actual business impact and impact to the Migration Plan.
- Status of the any risks, including those identified in the Risk Management Plan, as well as the steps being taken to mitigate such risks.

1.53 Exit Management / Transition-Out Services

- 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 department. It is the prime responsibility of Bidder/CSP during exit management period and in no way any facility/service shall be affected/degraded. Further, Bidder/CSP is also responsible for all activities required to train and transfer the knowledge to department (or representative agency of department).
- 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 Bidder/CSP. 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.
- At the end of the contract period or upon termination of contract, Bidder/CSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of department.

1.54 Exit Management Plan

- Bidder/CSP 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.
- Bidder/CSP shall provide support to department for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment RFP.
- Exit Management Plan will include following but limited to:
    - A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor 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.
    - Plans for the communication with such of the Bidder/CSP, 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.

- Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.
- Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
- Proposal for necessary setup or institution structure required at department level to effectively maintain the project after contract ending.
- Training and handholding of department Staff or designated officers for maintenance of project after contract ending.

▪ Department will approve this plan after necessary consultation and start preparation for transition.

1.55 Exit Management Services

▪ Bidder/CSP shall be responsible for copy of all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to department supplied industry standard media.

▪ Bidder/CSP shall retain the data / copy of Database for 90 days and Bidder/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.

▪ The format of the data transmitted from the Bidder/CSP to the department should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. Bidder/CSP must ensure that the virtual machine format is compatible with other Bidder/CSP, so that department can migrate from one Bidder/CSP to other Bidder/CSP. department should be able to export the virtual machine from Bidder/CSP cloud and use that anywhere. Bidder/CSP shall give provision to import cloud VM template from other Bidder/CSPs.

▪ Bidder/CSP shall necessary support for termination of network connectivity to / from other Bidder/CSPs (within India) if required

▪ Bidder/CSP shall ensure that all the documentation required by the department for smooth transition (in addition to the documentation provided by the Bidder/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

▪ Post exit all the data content should be removed to ensure that the data cannot be recovered.

▪ Bidder/CSP shall address and rectify the problems with respect to migration of the department application and related IT infrastructure during the transition.

- Bidder/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.
- At any time during the exit management period, the Bidder/CSP will be obliged to provide an access of information to department and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogs, archive data, Live data, policy documents or any other material related to implementation of IT Infrastructure Solution for department.
- Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule

1.56 Connectivity and Customer Premises Equipment features

1.57 WAN Connectivity Requirements

- Bidder/CSP shall provide end-to-end redundant P2P connectivity (Primary and Secondary links) to connect the DR Site.
- Bidder/CSP shall provide redundant P2P connectivity (Primary and Secondary links) to connect department offices with DC & DR
- Bidder/CSP has to provide redundant internet link in primary and DR site to access the application from department office and other locations.
- Bidder/CSP shall make sure provided redundant links from two different Service Providers (ISP), alternate routing paths facilitated at ISP backbone, redundant network devices etc. These two ISPs should not share same back end infrastructure. Redundancy in security and load balancers, in high availability mode, will be provided to facilitate alternate paths in the network.
- Bidder/CSP has to configure the network links in auto failover mode is the responsibility of the Bidder/CSPs.
- Identification and classification of at least the following classes of application types must be supported by the solution:
    - Client server and web-based applications
    - Antivirus Solution
    - Operating System and Client software patching solution
- The vendor should ensure that traffic is prioritized as per the listing given by department. The actual division could change over time as per requirement of department Vendor should be able to make changes as required by department.
- Bidder/CSP shall have provision of secure tunnel / links for data replication to provide secure data replication for DR services.
- Bidder/CSP shall provide Managed Anti-DDoS Services capable of handling at least 1 GB of DDoS Attacks in all the links.
- Bidder/CSP shall provide 'Clean Pipe' in all the links.

- Bidder/CSP shall provide 24 x 7 x 365 Service Window for Link Management Services. The support mechanism must be confirmed by the Bidder/CSP with response times.
- The Bidder/CSP shall assign a service manager for the duration of the Contract. This resource should be the "Single point of contact" for all service related matters for department and should be able to respond within the designated service window. The proposed "Service manager" should be a multi-skilled professional and supported by back-end support as required.
- The proposed solution should also provide self-service capabilities which gives configuration access to department team.
- Bidder/CSP shall be responsible for DNS / reverse DNS changes in the Internet connectivity as and when required.
- Bidder/CSP should provide a report based on the IP and application high consumption bandwidth.

1.58 SMS facility for department applications

The department currently has multiple applications which use the SMS facility for sending status updates to citizens, for login of department officers etc. The Bidder/CSP would procure and provide the SMS services to the department as per requirement. The Bidder/CSP can procure the service from the any of the service providers and charge a fixed rate to the department during the tenure of the contract. The Bidder/CSP must use the current SMS headers used by the department

1.59 VPN Service

The Bidder/CSP should provide VPN solution to enable the department field offices to access the department applications hosted on cloud in a secure manner and provide services to citizens. VPN service will be part of the package and will not be billed separately to department.

2. Cloud Security Requirement

The Bidder/CSP should ensure complete security requirements for the Government Community Cloud hosting of department with suitable security arrangements through SaaS model (Security as a Service) as per Meity guidelines. Bidder/CSP shall provide end-to-end security services to meet IT security challenges for the Infrastructure based on the proven frameworks and security best practices. It is vital for complete security that the processes and technology which shall support the Information Security function are proven and adhere to standards.

It is envisaged that the security operations shall be centralized, structured and coordinated and shall be responsive resulting in effective threat prevention and detection helping the deployed cloud solution to be secure from attackers. The Information Security functions shall respond faster, work collaboratively, and share knowledge more effectively. The proposed cloud solution shall have multiple security layers to secure the infrastructure from threats. Bidder/CSP shall propose and provide security solutions that may not be mentioned in the RFP but are required as per the guidelines of Meity.

Bidder/CSP shall provision for following security solutions (not limited to):

- Next-Generation Firewall (NGFW) having minimum 2 Gbps threat-prevention throughput (all features enabled).
- Web Application Firewall for OWASP (Open Web Application Security Project) Top 10 p9rotection
- IPS (Intrusion Prevention System)/IDS (Intrusion Detection System)
- HIPS (Host Intrusion Prevention System)
- Malware Analysis - Bidder/CSP shall conduct analysis of newly discovered malware to uncover its scope and origin.
- DDoS (distributed denial-of-service) service - Bidder/CSP would offer DDOS Protection to protect the cloud infrastructure and application from well-equipped attackers. Minimum mitigation of 1 Gbps.
- Anti-Virus - This Service includes virus detection and eradication, logon administration and synchronization across servers, and support for required security classifications.
- IDAM (Identity Access Management) - The User Management services shall include Directory Services for which comprises of the following services:
    - Domain management
    - Group management
    - User management
    - Implementation of domain policies and standards etc.
    - Directory services are to be used by department.
    - Role Management
    - Access Management
    - Multi-Factor Authentication

    - Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.
- SIEM - The Bidder/CSP shall also propose for Security Information and Event Management (SIEM) solution supporting threat detection and security incident response through the real-time collection and historical analysis and correlation of security events from a wide variety of event and contextual data sources. It shall also support compliance reporting and incident investigation through analysis of historical data from these sources.
- VAPT (Vulnerability Assessment and Penetration Testing) – The Bidder/CSP shall conduct vulnerability and penetration test (from a third-party testing agency which has to be CERT-IN empanelled) on the Cloud facility every 6 months and reports shall be shared with department. The Bidder/CSP needs to update the system in response to any adverse findings in the report, without any additional cost to department.
- Security solution during data in transit and at rest
- Anti-APT (Advanced persistent threat) Solution – It shall Identify and analyse targeted and unknown files for more than 100 malicious behaviours. IT shall generate and automatically deliver protection for newly discovered malware via signature updates.
- NTP (Network Time Protocol) - Clock Synchronization - The provisioned NTP solution should have the capability to synchronize clock with systems like network equipment, voice systems, servers, appliances, desk top systems etc

It is critical to have a set of IT security management processes and tools to ensure complete security of cloud solution. An IT security policy, framework and operational guidelines as per ISO 27001, 27017, 27018 & PCI-DSS be maintained & implemented by Cloud service provider (Bidder/CSP).

Department will perform physical audits at the data centre and will require access to the department's infrastructure as and when required by department.

All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.

Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of department.

Cloud service shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.

2.2Security Controls

- Bidder/CSP shall provide adequate security controls not limited to the measures as described below:
- Secure Access Controls
    - The system shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.
- Authorization Controls

- A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.

- Logging
  - Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance to the least privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.
- Hardening
  - All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted and all known insecure protocols shall be disabled.
- Malicious Software Prevention
  - Implementation of anti-virus software and other malicious software prevention tools shall be supported for all applications, servers, data bases etc.
- Network Security
  - The network architecture must be secure with support for UTM, Firewall and encryption. The system shall also allow host-based firewalls to be configured, as an additional layer of security if the network firewall were to fail.
  - Cloud services shall be provided on a 10Gbps scalable to 50Gbps network connectivity between the server and Storage and Network. Cloud service shall be able to support multiple (primary and additional) network interfaces. The proposed data center shall be isolated from failures in other data centers. As mentioned in RFP Bidder/CSP proposed data center shall be connected with low latency and in-expensive network connectivity.
  - Cloud service provider should able to configured the secure network over an internet like IPsec VPN tunnel or SSL VPN.
  - Cloud services shall provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud and also provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.
- Information Security: Log Monitoring and Correlation
  - All Servers / sub systems / network devices / appliances as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, security component / devices of the system shall be monitored. Bidder/CSP must provide a Security information and event management (SIEM) solution for the same which shall be capable to provide various security alerts, events, logs generated from various IT infrastructure (Hardware/Software) components. Bidder/CSP would need to ensure the IT security compliance and therefore monitor the threats/logs generated by various equipment's / sub systems.
  - The Bidder/CSP would need to store the events for minimum 6 months. Also, Bidder/CSP will be required to scale the storage if the existing storage space is full.

2.3 Cloud Security Administration

- The Bidder/CSP shall provide 24x7x365 managed services for the entire security stack protecting the department environment. Bidder/CSP shall be responsible for managing configuration and patch management, vulnerability scanning, protecting data in transit and at rest, managing credentials, identity, and access management etc. The activities include:
  - Appropriately configure the security groups in accordance with the Security policies
  - Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
  - Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
  - Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity
  - Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Agency's policies
  - Review the audit logs to identify any unauthorized access to the government agency's systems.
  - The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by Bidder/CSP.
  - Service Component Administration
  - User and Password Control
  - Check and maintain access control
  - Routine connection tests
  - Change & Configuration Management
  - IP / Port / Zone Configuration
  - Firewall policy / IPsec VPN / SSL VPN configuration
  - NAT / PAT configuration
  - Multicast configuration
  - Antivirus / IPS Signature update, when released by vendor
  - Fault Management
  - Response to alerts generated by systems or problems reported.
  - Troubleshooting, root cause analysis (RCA) and identification of problem area
  - Resolution of problems through configuration changes/ re-installations / replacements
  - Escalate hardware failures to hardware vendor
  - Assist hardware vendor to Identify problem area (by log collection & reboot)
  - Log Storage: Store critical logs in shared Syslog server for retention period of 90 days
  - Configuration backup: Take incremental configuration backup daily for retention period of 90 days and Restoration of configuration when required.
  - Trouble ticket logging, update, and closure
  - Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise department about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.

- Incident Response - The Bidder/CSP should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The Bidder/CSP/Bidder/CSP must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.
- Governance & Risk Assessment - The Bidder/CSP should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.

3. Bidder/CSP Technical and Functional Compliance

3.1 Cloud Portal

Sr.	Cloud Capabilities	Compliance(Y/N)
1	In order to increase the service availability, the cloud service provider must offer multidimensional auto-scaling of cloud services where resource like RAM and CPU will scale vertically as well systems should scale horizontally	
2	Cloud service should enable to provision cloud resources through self service provisioning interface.	
3	Cloud System should enable to provision cloud resources from application programming interface (API)	
4	Cloud System should be accessible via secure method using SSL certificate.	
5	Should be able to create, delete, shutdown, reboot virtual machines from Cloud portal.	
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines	
7	Should be able to predict billing of resources before provisioning any cloud resources if integrated with billing system.	
8	Should be able to set threshold of cloud resources of all types of scalability.	
9	Should be able to provision any kind of resources either static or elastic resources.	
10	The cloud virtual machine created by portal should be have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.	
11	The Cloud System shall be capable of allowing applications to self-service compute, network and storage infrastructures automatically based on workload demand.	
12	Should ensure that the virtual machine format is compatible with other cloud systems.	

13	Cloud System should give provision to import cloud VM template from other cloud systems.	
14	Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.	
15	Cloud System should give provision to attached new block disk to any cloud VM from self-service portal.	
16	The cloud virtual machines should be scalable in terms of RAM and CPU automatically without reboot.	
17	Cloud System must support multi-tenancy for management perspective. Different department or group company should be able to access allocated resources only.	
18	The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User Departments.	
19	The Solution should provide Unified Infrastructure management with complete inventory management of virtual machines & physical resources.	
20	The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services.	
21	Cloud System should have provision to ensure that cloud virtual machine is into separate network tenant and virtual LAN.	
22	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM	
23	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM.	
24	Cloud System must ensure the ability to map private IP address of cloud VM to public IP address as require from portal of Cloud Orchestration System.	
25	Should ensure that cloud VM network is IPV6 compatible.	
26	Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.	
27	Cloud Orchestration System should provide network information of cloud virtual resources.	

28	Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control	
29	Cloud System should support policy based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example if any users doesn't have permission to delete VM, he should not be able to do it.	
30	Cloud System should support quota based system. Users should not be able to provision resources beyond allocated quota.	
31	The Admin should be able to define Access Control to Permit or Deny operation per Group or per User.	
32	Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.	
33	The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud datacenter.	
34	User Management: The solution shall provide comprehensive user management	
35	Functions including tenant-specific user grouping and admin/user rights within the scope of a tenant. The tenant-admin user is considered distinct from the overall cloud solution administrator. The tenant-admin shall be able to manage own profile, tenant preferences, as well as users within the tenant/group scope. Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the rights to all User Management functions.	
36	Cloud System should provide facility to make template from virtual machines.	
37	Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.	
38	Cloud System should have provision to live migration of virtual machine to another physical servers in case of any failure.	
39	Cloud System should have provision to migration of virtual machine from one hypervisor platform to another hypervisor platform through its UI.	

40	Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.	
41	The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.	
42	The Cloud System cloud solution should support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.	
43	The solution shall provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.	
44	Cloud System should give provision to monitor the network traffic of cloud virtual machine.	
45	Cloud System should offer provision to analyse of amount of data transferred of each cloud virtual machine.	
46	Cloud System must offer provision to monitor uptime of each cloud virtual machine.	
47	Cloud System 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.	
48	Cloud System must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.	
49	Cloud System must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.	
50	Cloud System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.	

51	Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.	
52	Cloud System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity	
53	Should be able to create virtual instances of required configuration without limiting to any standard templates	

3.2General Cloud Requirement

#	Description	Compliance(Y/N)
1	Department intends to avail a managed Meity Government Community cloud for hosting The application at the Bidder's Data-Center.	
2	The data-centre shall be at least an Uptime/TIA 942 certified Tier III data-centre providing 99.982% services availability SLAs	
3	The data-centre shall be well equipped with physical, logical, network and infrastructure security solutions, access protection systems including physical access control, and shall maintain the logs of the access.	
4	The data-centre shall be 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 department Web, App and DB environment	
5	The data-centre shall have ability to scale up or down the servers/compute resources on-demand/ as desired without significant down time.	
6	The compute infrastructure shall include the physical / virtual machines, operating systems, application servers, database server, anti-virus solutions and system management & back-up agents.	
7	The IT infrastructure should be hosted on Government Community	

8	All the virtual machines should be auto scalable in terms of RAM	
9	The cloud platform should be enough intelligent to predict incoming load and assign resources to virtual machines dynamically without rebooting system.	
10	Cloud platform should always allocate minimum 50% buffer resources against running load to handle sudden spikes.	
11	The cloud platform should provide high availability across virtual machines so that even if any host goes down, all guest virtual machines should be migrated	
12	Cloud platform should support horizontal load balancing along with vertical. Load balancer should be used to load balance traffic. Load balancer should be able to trigger new virtual machines to handle additional load. If load goes down, newly triggered virtual machines should be recycled.	
13	Cloud provider should give department a dashboard of all virtual machines to monitor allocated and used resources by APPLICATION and associated applications.	
14	Cloud dashboard should allow to generate reports for trend analysis of system usage.	
15	Department team should be able to get the console access of any virtual machines if require.	
16	There should be provision to generate historical reports of resources utilization.	
17	There should be admin panel to create, delete, start, stop, and copy virtual machines.	
18	There must be provision to create golden image of virtual machine so that it can be used to make more machines of same configuration.	
19	There should be provision to take snapshots of machines so that working images of testing/quality	

20	Bidder/CSP should provide a VPN solution to the enable the department field offices to access the department applications hosted on cloud in a secure manner. The solution should enable the field offices with poor connectivity/ no connectivity to access the department applications and provide services to citizens	
21	Bidder/CSP should procure the service from the any of the service providers and charge a fixed rate to the department during the tenure of the contract. The Bidder/CSP must use the current SMS headers used by the department	

3.3 Cloud Portal Service Provisioning

Sr.	Description	Compliance Y/N
1	The Service provider should offer cloud service provisioning portal for in order to provision cloud services either via portal, mobile app or automated using	
2	Cloud service provider should enable to provision / change cloud resources through self service provisioning portal.	
3	Service provider should enable to provision / change cloud resources from application programming interface (API).	
4	The user admin portal should be accessible via secure method using SSL	
5	Should be able to take snapshot of virtual machines from provisioning portal.	
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines.	
7	Should be able to predict his billing of resources before provisioning any cloud resources.	

8	Department should be able to set threshold of cloud resources of all types of scalability.	
9	Should be able to provision all additional storages required for cloud services.	
10	Should be able to provision any kind of resources either static or elastic resources.	
11	Should get list of all cloud resources from provisioning	
12	Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.	

3.4Web Application Firewall (WAF)

#	Description	Compliance (Y/N)
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection	
2	Service provider WAF should be able to support multiple website security.	
3	Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.	
4	Service provider WAF should be able to block invalidated requests.	
5	Service provider WAF should be able to block attacks before it is posted to website.	
6	Service provider WAF should have manual control over IP/Subnet. i.e., Allow or Deny IP/Subnet from accessing website.	
7	The attackers should receive custom response once they are blocked.	
8	Service provider must offer provision to customize response of vulnerable requests.	
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10	Service provider WAF should be able to Whitelist or Backlist IP/Subnet.	

11	Service provider WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceed the threshold limit.	
12	The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.	
13	WAF should be able to set a limit to maximum file size, combined file size in bytes	
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions & headers	
15	Service provider WAF should be able to limit maximum number of arguments, argument name, value, value total length etc.	
16	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.	
17	Should be able to limit maximum size of request body entity in bytes	
18	The WAF should be able to close all the sessions of an IP if it is ban.	
19	Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.	
20	The WAF access and security Dashboard should show a graphical representation of	
	A) For access report analysis purpose the Dashboard should contain following information:	
	i) Number of hits by status code	
	ii) HTTP status code wise hits	
	iii) HTTP methods wise hits	
	iv) Client browser wise hits	
	v) Client Operating system wise hits	
	vi) Traffic(No. of hits) per URL	
	vii) Average bytes received per request	
	viii) Average bytes sent per request	
	ix) Average time elapsed per request	

	B) For security report analysis purpose the Dashboard should contain following information:	
	i) Average score by status code	
	ii) Distribution of blocked requests	
	iii) Number of blocked requests	
	iv) OWASP Top 10 requests	
	v) Reputation tags	
	vi) IP list reputation	
	C) For network incoming and outgoing traffic captured by WAF packet filter dashboard should contain following information:	
	i) Number of packet hits	
	ii) Source IP, Destination IP wise hits	
	iii) Firewall actions(allow, deny) wise hits	
	iv) Requests per destination port wise hits	
	D) Geo map of number of hits by country	
21	WAF should support different policies for different web applications.	
22	Vendor to ensure 24x7x365 availability of WAF service.	
23	WAF should support different policies for different application section (different security zones within the app).	
24	WAF should support IP Reputation DB (DB including blacklisted IP Address, IP Address, Anonymous Proxy, Botnets, Windows Exploit etc.) along with Client Source IP address based Security Policy and dynamic source IP blocking.	
25	WAF should enforce file upload control based on file type, size etc.	
26	WAF should detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses or anonymous proxy addresses.	
27	WAF should support detection only, blocking and transparent mode.	
28	WAF solution should be capable of handling IPV4 and IPV6 traffic.	

29	WAF solution should ensure compliance and advanced protection against industry standards such as OWASP Top 10 vulnerabilities etc.	
30	Vendor must monitor, manage & maintain the WAF solution on a 24x7 basis.	
31	WAF should provide a real-time dashboard with data such as top attacks view, traffic monitoring view, etc.	
32	WAF should provide role based access control for the dashboard (role based multiple login accounts both primary and secondary to be provided).	
33	WAF should provide detailed reports for all web application attacks.	
34	WAF should be able to decrypt the SSL traffic to analyse the HTTP data and should be able to re-encrypt the SSL traffic.	
35	WAF should support SSL offloading.	
36	WAF should support body inspection, content injection, backend compression, validation of UTF8 Encoding, XML Inspection.	
37	WAF should block invalid BODY.	
38	WAF should log all transactions for auditing purpose.	
39	WAF should block desktop users User-Agent, crawlers User-Agent, suspicious User-Agent.	
40	WAF should have customizable scoring policy for each request and can block request if global score exceeds.	
41	WAF should have DOS and BF protection for all or specific URLs.	
42	WAF should have learning mode to create whitelist/blacklist rules and also block attack in learning mode.	
43	WAF should verify SSL certificate, certificate name, expiration and cipher suites. Also control over accepted TLS/SSL protocol, cipher order, CRL verification, HTTP public key pinning, OBidder/CSP stapling.	
44	WAF should allow to inject Request and Response headers for applications.	
45	WAF should support Content and URL rewriting policies.	

46	WAF should send proxy HTTP headers to backend, r rewrite cookie path, backend' s cookies encryption and override backend server HTTP errors.	
47	WAF should support force HTTP to HTTPS redirection.	
48	WAF should support URL specific rulesets and should allow/deny specific countries(GeoIP) for applications.	
49	WAF should have OS level firewall to PASS/BLOCK traffic inbound/outbound traffic	
50	WAF should allow to create custom rules for application.	
51	WAF should support Active-Active/Active-Passive failover.	

3.5 DRM Tool

#	Description	Compliance Y/N
1	The proposed solution should provide a single dashboard for Heterogeneous Environments including physical Virtual and Cloud Environments	
2	The proposed solution should support Provisioning systems and closely integrated with private / public cloud	
3	The proposed solution should provide Application / Business impact analysis from application perspective which may help understanding revenue loss, regulatory loss, cost of downtime, reputation loss to make informed business decision	
4	The proposed solution must offer real time visibility of a DR solution parameters like RPO, RTO, Maximum Tolerable Period of Disruption (MTPoD), Application Health, replication status and should provide alerts on any deviations	
5	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion and firewall policy and custom application monitoring services etc. to ensure DR readiness	
6	The proposed solution should allow monitoring basic health parameters for DC & DR components using SNMP	

7	The proposed solution should provide capable of recovering multiple systems parallel and support inbuilt load balancing techniques for optimized recovery	
8	The proposed solution should be capable of Recovering Servers, Storage, Network, Application, DB, Webserver and Middleware layers on a click of a button	
9	The proposed solution should facilitate Ready to use solution packages for cross platform recovery	
10	The proposed solution should not rely on scripting for recovery automation	
11	The proposed solution should allow automating process document and storing it over the cloud / across data centre and provide to track through mobile and/or email	
12	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication	
13	The proposed solution should provide API's for Hypervisor integration and automate various actions pertaining to virtual servers	
14	The proposed solution should provide out of the notification manager to provide alerts through SMS, email, etc. in case of threshold breach or threat of SLA violation	
15	The proposed solution if required, should provide out of the box exception handling manager which may allow taking remedial action in response to certain alerts/alarms	
16	The proposed solution should provide out of the box reports on RPO deviation, RTO deviation, Data lag, Application DR Readiness status and replication trending	
17	The proposed solution should provide DR drill and audit reports compliant to ISO 22301 standard and/or requirements of the Department	
18	The proposed solution should be capable of generating reports in pdf, csv, XML format	

19	The proposed solution must support all major platforms including Linux, Windows, Solaris, Unix with native high availability options. It must support both physical and virtual platforms.	
20	The proposed solution must have pre-packaged support for all popular databases Oracle, PostGres SQL, MSSQL, Sybase and DB2	
21	The proposed solution should integrate with applications/databases using pre-fabricated API's	
22	The proposed solution should have granular, role based administration and should use existing Active Directory/LDAP, SAML for authentication without the need of its own separate identity management database	
23	The proposed solution should provide completely agentless approach for DR monitoring and automation	
24	No Production down time should be requested for Installation/integration/configuration of the proposed management Product	
25	The proposed IT Disaster Recovery Manager should be capable of integrating with Business Continuity Management solutions	

3.6Vulnerability Assessment and Monitoring Service

#	Description	Compliance Y/N
1	Monitoring of Web Applications including the corporate websites etc., and protect it from malicious mobile codes like computer viruses, worms, Trojan horses, spyware, adware, key-loggers and other malicious programs. The service should be Non- Intrusive in nature.	
2	Malware Monitoring scanning should be performed on Daily basis. If any malware is injected into Web Applications, then immediate malware alert message is forwarded to the stake-holders. Application Audit and Vulnerability assessment on weekly basis to ascertain if any corrective action needs to be taken in application based on any observations found in the scanning.	

3	Should be able to detect malicious code injection/links, both known and unknown malware, Web-page tampering, various zero-day browser exploits etc.	
4	Should be able to identify the malware source, malware threat area and coverage, encoded Java Script and VB script and should not rely on pattern/signature-based technology.	
5	It should have minimal impact on traffic, server performance, networks etc. during deployment and operation	
6	Should be able to work in any network topology.	
7	Should be able to identify applications running on non-standard ports	
8	Should have configurable scan intervals (frequency), Configurable notification, alerting and reporting options, Configurable "whitelist" option for allowed links, Configurable scan schedules and on-demand scans.	
9	Should have Real-time instant alerting upon detection of malicious behaviour (Email or SMS).	
10	Should have detailed remediation recommendation guidance including step by step instructions on how to address the threats captured.	
11	Should have On demand Vulnerability Scanning without user intervention	
12	Should Perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).	
13	Should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to : Windows, AIX, UNIX, Linux, Solaris servers etc.	
14	Should be able to perform authenticated and unauthenticated scans	
15	Should be able to detect weak password.	
16	Should be able to identify out-of-date software versions, applicable patches and system upgrades	
17	Should Flag the presence of any blacklisted software	

18	Should be able to perform On demand Application Audit for all types of websites including AJAX, WEB2.0, and obfuscated Java Script etc. and identifies vulnerabilities throughout the entire application, scanning the browser and server-side components.	
19	Should check regularly for Defacement Detection, websites changes and detect for possible defacement. Such daily defacement checks protect the brand, credibility and reputation of the bank.	
20	Should have a Executive Dashboard that provides a comprehensive synopsis of reported vulnerabilities and malware, remediation suggestions as well as several alert and support options in predefined report formats. It should have Role based access.	
21	Should be able to provide remediation information in the reports including links to patches etc.	
22	Should be able to produce a report listing all applications on a host or network, regardless of whether the application is vulnerable	
23	Should Include a library of potential vulnerabilities and rules which covers SANS (SANS Institute) top 20. This library should be customizable by administrator and changes to the same are to be traceable.	
24	Provide detailed report as spreadsheet, PDF and HTML format, customizable as per the requirement and comparable to previous assessment.	
25	Should be able to generate reports on trends in vulnerabilities on a particular asset.	
26	Should have Scan history and comparison provided in Scan Report.	
27	Should have banner grabbing feature which tries to discover web-applications in the domain.	
28	Should Support industry standard reporting including OWASP top 10 categories.	
29	Should support authenticated scanning with different authentication methods including	
	Form, HTTP basic, NTLM and digest.	
30	The web application vulnerability scanning module should be able to identify the following vulnerabilities but not limited to in the underlying application.	
	· XSS	

	· Form Validation	
	· Block Malformed content	
	· Back Doors	
	· Spoofing	
	· SQL injection	
	· Directory/path traversal	
	· Forceful browsing	
	· LDAP injection	
	· SSI injections	
	· XPath injection	
	· Sensitive information leakage	
31	Should support domain reputation in Google, SURBL, Malware Patrol, Clean-Mx, Phishtank	
32	Should be able to check mail server IP and check in multiple RBL repositories	
33	Should be able to scan SQL Injections for My SQL, MSSQL, PostGres SQL, Oracle databses	
34	Should be able to scan Local file inclusion (LFI) , Remote file inclusion (RFI) , XSS - Cross Site Scripting & Malware.	
35	The scanning should support\cover following	
	· Open ports scanning for Security Threats	
	· Banner detection, directory scanning & directory indexing.	
	· Full Path disclosure in the pages	
	· Password auto complete enabled fields	
	· Page defacement detection & view state decoder	
	· Password submission method	
	· Time based scanning	
	· Robust link crawler	
	· SSL Certificate checking	
	· Web Shell Locater & Web Shell Finder	
	· Reverse IP domain check	
36	Generate logs for scanner access and testing.	
37	Solution should be a tool based automated solution	
38	Solution should support scanning of static and dynamic links	
39	Solution should be independent of application platform	

40	Malware Monitoring scanning on hourly basis. If any malware is injected into Web Applications, then immediately malware alert message shall be forwarded to authority. Application Audit and Vulnerability assessment of weekly basis.	
41	It should be able to integrate with other security solutions (i.e. Security Information / Event Management, Patch Management, IDS, IPS, etc.)	
42	It should integrate with the existing / proposed WAF solution	
43	24*7 monitoring / scanning of web pages for real time detection of malware injection. No skipping of page scanning.	
44	The service provider should have the ability to provide/Create Users with various privilege levels (view only / View or take down certain incident types)	

3.7 Application Performance Monitoring

#	Database Monitoring	Compliance Y/N
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, RECONFIGURE Configurations, Memory Configurations)	
6	Bandwidth utilization, latency, packet loss etc.	
7	APM should be able to provide Jobs and Backup Details, including the following:	
	i) Currently executing Jobs.	
	ii) Job Steps Execution Info.	
	iii) Job Schedule Info.	
	iv) Recent Database Backup.	
	v) Back-Up within Past 24 Hours.	

8	APM should monitor and provide details on the following queries performance parameters:	
	i) Top Queries by CPU , Top Queries by I/O	
	ii) Top Waits by Waiting Tasks , Top Slow Running Queries	
	iii) Most Frequently Executed Queries, Most Blocked Queries	
	iv) Top Queries by Lowest Plan Reuse, Cost of Missing Indexes	
9	APM should provide to set following monitoring parameters for continuous monitoring:	
	i) Total Server Memory, SQL Cache Memory	
	ii) Optimizer Memory, Lock Memory	
	iii) Connection Memory, Target Server Memory	
	iv) Granted Work Space Memory, Buffer Cache Hit Ratio	
	v) Page Lookups/Sec, Pages Read/Sec	
	vi) Page Life Expectancy (ms)	
	vii) User Connections, Logins/Sec	
	viii) Logouts/Sec, Cache Hit Ratio	
	ix) Cache Count, Cache Pages	
	x) Lock Requests/Sec, Lock Wait/Sec	
	xi) Lock Timeout/Sec , Full Scans/Sec	
	xii) Range Scans/Sec, Probe Scans/Sec	
	xiii) Work Files Created/Sec, Work Tables Created/Sec	
	xiv) Index Searches/Sec, Latch Waits/Sec	
	xv) Average Latch Wait Time, Batch Requests/Sec	
	xvi) SQL Compilations/Sec, SQL Recompilations/Sec	
	xvii) Auto-Param Attempts/sec, Failed Auto-Params /Sec	
	xviii) Safe Auto-Params/Sec, Unsafe Auto-Params/Sec	
	xix) Availability	

#	Web Service Monitoring	Compliance (Y/N)
1	APM should provide website details hosted on web server.	
2	APM should provide application details running on web server.	
3	Monitoring & management of network link proposed as part of this	
4	Bandwidth utilization, latency, packet loss etc.	
5	APM should consist of the following monitoring parameters:	
	i) Site Status, Total Bytes Sent	
	ii) Bytes Sent/Sec, Total Bytes Received	
	iii) Bytes Received/Sec, Total Bytes Transferred	
	iv) Bytes Total/Sec, Total Files Sent	
	v) Files Sent/Sec, Total Files Received	
	vi) Files Received/Sec, Current Connections	
	vii) Maximum Connections, Total Connection Attempts	
	viii) Total Logon Attempts, Service Uptime	
#	**Application**	**Compliance Y/N**
1	APM should consist of the following monitoring parameters:	
	i) Memory Monitoring	
	ii) Web Applications and Deployments	
	iii) Connections, Transactions, Queries	
	iv) Web Metrics	
	v) Transactions	
	vi) Availability	
2	Monitoring & management of network link proposed as part of this solution.	
3	Bandwidth utilization, latency, packet loss etc.	

3.8SIEM Service

#	SIEM Description	Compliance (Y/N)
1	The solution should be able to handle events equal to the events handled by current system	
2	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.	

3	The solution should be capable of real time analysis and reporting.	
4	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
5	The solution should be able to assign risk scores to your most valuable asset. The risk value could be assigned to a service, application, specific servers, a user or a group. The solution should be able to assign and consider the asset criticality score before assigning the risk score.	
6	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.	
7	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.	
8	The SIEM receiver/log collection appliance must be an appliance based solution and not a software based solution to store the data locally, if communication with centralized correlator is unavailable.	
9	The solution should be able to collect logs via the following ways as inbuilt into the solution: Syslog, OPSec, agent-less WMI, RDEP, SDEE, FTP, SCP, External Agents such as Adiscon.	
10	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
11	The solution should provide a data store which is compressed via flexible aggregation logic.	
12	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.	
13	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.	
14	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.	
15	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.	

16	The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.	
17	A well-defined architecture along with pre and post installation document need to be shared by the bidder.	
18	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.	
19	The solution should support collection of events/logs and network flows from distributed environment(s).	
20	The solution should correlate security/network events to enable the SOC to quickly prioritize it's response to help ensure effective incident handling.	
21	The solution should integrate asset information in SIEM such as categorization, criticality and business profiling and use the same attributes for correlation and incident management.	
22	The solution should provide remediation guidance for identified security incident:	
23	Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis/remediation.	
24	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.	
25	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
26	The solution should perform regular (at least twice a year) health check and fine tuning of SIEM solution and should submit a report.	
27	The solution should share the list of out of the box supported devices/log types.	
28	The solution should support hierarchical structures for distributed environments. The solution should have capability for correlation of events generated from multiple SIEM(s) at different location in single management console.	

29	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
30	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP (User Datagram protocol) or similar ports should not be used.	
31	Event dropping/caching by SIEM solution is not acceptable and same should be reported and corrected immediately.	
32	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.	
33	The solution should be able to capture all the fields of the information in the raw logs.	
34	The solution should support storage of raw logs for forensic analysis.	
35	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	
36	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
37	The solution should support configurable data retention policy based on organization requirement.	
38	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.	
39	The solution should compress the logs by at least 70% or more at the time of archiving.	
40	The solution should have capability for log purging and retrieval of logs from offline storage.	
41	Solution should be capable of replicating logs in Synchronous as well as Asynchronous mode for replication from Primary site to DR site.	
42	The solution should provide proactive alerting on log collection failures so that any potential loss of events and audit data can be minimized or mitigated.	

43	The solution should provide a mechanism (in both graphic and table format) to show which devices and applications are being monitored and determine if a continuous set of collected logs exist for those devices and applications.	
44	The solution should support automated scheduled archiving functionality into file system.	
45	The solution should support normalization of real time events.	
46	The solution should provide a facility for logging events with category information to enable device independent analysis.	
47	The platform should be supplied on Hardened OS embedded in Hardware / Virtual Appliance. The storage configuration should offer a RAID configuration to allow for protection from disk failure.	
48	The platform should have High Availability Configuration of necessary SIEM components to ensure there is no single point of failure. Please describe the architecture proposed to meet this requirement.	
49	By default at the time of storage, solution should not filter any events. However, solution should have the capability of filtering events during the course of correlation and report generation.	
50	The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.	
51	The solution should be able to continue to collect logs during backup, de-fragmentation and other management scenarios.	
52	The solution should support collection of logs from all the devices quoted in RFP.	
53	The collection devices should support collection of logs via the following but not limited methods:	
54	1. Syslog over UDP / TCP	
55	2. SNMP	
56	3. ODBC (to pull events from a remote database)	
57	4. FTP (to pull a flat file of events from a remote device that can't directly write to the network)	
58	5. Windows Event Logging Protocol	
59	7. NetBIOS	

60	The solution should allow a wizard / GUI based interface for rules (including correlation rules) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.	
61	The solution should support all standard IT infrastructure including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, LDAP, Internet Gateway, Antivirus, and Enterprise Messaging System, Data loss prevention (DLP) etc.	
62	Solution should have license for minimum 10 users for SIEM administration.	
63	The solution should have the ability to define various roles for SIEM administration, including but not limited to: Operator, Analyst, SOC Manager etc. for all SIEM components.	
64	The solution should support SIEM management process using a web based solution.	
65	The solution should support the following co- relation: ▪ Statistical Threat Analysis - To detect anomalies. ▪ Susceptibility Correlation - Raises visibility of threats against susceptible hosts. ▪ Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities ▪ Rules based Correlation - The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios.	
66	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts.	
67	The solution should provide ready to use rules for alerting on threats e.g., failed login attempts, account changes and expirations, port scans, suspicious file names, default usernames and passwords, High bandwidth usage by IP, privilege escalations, configuration changes, traffic to non-standard ports, URL blocked, accounts deleted and disabled, intrusions detected etc.	

68	The solution should support the following types of correlation conditions on log data: a) One event followed by another event b) Grouping, aggregating, sorting, filtering, and merging of events. c) Average, count, minimum, maximum threshold etc.	
69	Solution should provide threat scoring based on: a) Host, network, priority for both source & Destination b) Real-time threat, event frequency, attack level etc.	
70	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.	
71	The solution should have the capability to send notification messages and alerts through email, SMS, etc.	
72	The solution should support RADIUS and LDAP / Active Directory for Authentication.	
73	The solution should provide highest level of enterprise support directly from OEM.	
74	The solution should provide a single point of contact directly from OEM for all support reported OEM.	
75	The solution should ensure continuous training and best practice updates for onsite team from its backend resources.	
76	Solution should support log integration for IPv4 as well as for IPv6.	
77	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert/retrieval time, resource utilization details etc.	
78	Solution should support at least 100 default correlation rules for detection of network threats and attacks. The performance of the solution should not be affected with all rules enabled.	
79	The central management console/ Enterprise Security managers/receivers should be in high availability.	
80	24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	
81	Recording and analysing data sources (e.g. system status, failed authentication attempts, etc.)	

82	24/7 contactable security incident handling and troubleshooting team with the authority to act	
83	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	
84	Provision of relevant log data in a suitable form	
85	Logging and monitoring of administrator activities	

4. Existing BoQ

4.1 IGR DC

Env.	Hosting Components	Quantity
A.1	**Cloud Hosting**	**Unit**
Application & DB servers	vCores: 4 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Windows 2012 R2| DB:	26 NO
	vCores: 32 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2520 GB | OS: RHEL 7.2| DB: PostgreSQL CE	4 NO
	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: Windows 2012 R2| DB:	3 NO
	vCores: 8 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 350 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 48 | RAM: 128 GB | Usable Performance Storage (800-1200 IOPs/TB): 2757.6 GB | OS: Windows 2012 R2| DB: MSSQL Enterprise 2014	1 NO
	vCores: 2 | RAM: 4 GB | Usable Performance Storage (800-1200 IOPs/TB): 100 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 2 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 100 GB | OS: Windows 2012 R2| DB:	3 NO
	vCores: 24 | RAM: 128 GB | Usable Performance Storage (800-1200 IOPs/TB): 29000 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 38 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1843.2 GB | OS: RHEL 7.2| DB: PostgreSQL CE	1 NO
	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 1000 GB | OS: RHEL 7.2| DB:	1 NO
	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 600 GB | OS: RHEL 7.2| DB: PostgreSQL CE	2 NO
	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: RHEL 7.2| DB:	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1000 GB | OS: RHEL 7.2| DB:	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 600 GB | OS: RHEL 7.2| DB: PostgreSQL CE	1 NO
	vCores: 4 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 720 GB | OS: RHEL 7.2| DB: PostgreSQL CE	1 NO
	vCores: 32 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1980 GB | OS: RHEL 7.2| DB: PostgreSQL CE	1 NO
	vCores: 4 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 600 GB | OS: RHEL 7.2| DB: PostgreSQL CE	1 NO

	vCores: 4 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 500 GB | OS: RHEL 7.2| DB:	1 NO
	vCores: 4 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: RHEL 7.2| DB:	1 NO
A.2	**Software Licenses**	**Unit**
OS	Windows Server	52 NO
	RHEL	16 NO
DB	PostgreSQl CE	11 NO
	MS SQL Enterprise 2014	24 NO
Monitoring Tool	Monitoring tool for VMs, Ports & Firewall	71 NO
A.3	**Backup & Storage Solution**	**Unit**
Backup	Backup (Space+Software)	18 TB
Storage	Additional Backup Storage (for File Share)	20.5 TB
A.4	**Network & Connectivity Services**	**Unit**
Services	vLoad Balancer (1 Gbps Throughput)	14 NO
	Public IP's	26 NO
	Cross Connect + Port Termination	2 NO
	Unmetered Internet Bandwidth at Datacenter Site	200 Mbps
A.5	**Security Services**	**Unit**
Services	vFirewall (1 Gbps Throughput)	4 NO
	vUTM (1 Gbps Throughput)	1 NO
	SIEM Tool	57 NO
	DDOS As a Service	1 NO
	Antivirus & HIPS	52 NO
	SSL Certificate (DV+OV)	13 NO
	Vulnerability Assesment test (Yearly Twice)	2 NO
	VPN (2 Factor Authentication)	500 NO
A.6	**Managed Hosting Services**	**Unit**
Services	Operating System Management Services	52 NO
	Storage Management Services	1 NO
	Backup Management Services	52 NO
	DB Management Services	8 NO
	vFirewall & vUTM Management Services	5 NO
	vLoad Balancer Management Services	14 NO

4.2IGR DR

Env.	Hosting Components	Quantity
A.1	**Softwares**	**Unit**
Monitoring Tool	Monitoring Tool	5 NO
A.2	**Storage Solution**	**Unit**
Storage	Near DR Storage	42 TB
	Far DR Storage	42 TB
A.3	**Network & Connectivity Services**	**Unit**
Services	Cross Connect + Port Termination	2 NO
	Unmetered Internet Bandwidth at Datacenter Site	100 Mbps
	Shared P2P Link from DC to DR	100 Mbps
	ILL for Far DR (For Redundancy)	100 Mbps
A.4	**Security Services**	**Unit**
Services	vFirewall (1 Gbps Throughput)	4 NO
	vUTM (1 Gbps Throughput)	1 NO
	DDOS As a Service	1 NO
A.5	**Managed Hosting Services**	**Unit**
Services	Storage Management Services	1 NO
	vFirewall & vUTM Management Services	5 NO
	DR Drill (Yearly Twice)	2 NO

4.3LR DC

Env.	Hosting Components	
A.1	**Cloud Hosting**	**Unit**
Application & DB servers	vCores: 4 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: Windows 2012 R2| DB:	3 NO
	vCores: 12 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Windows 2012 R2| DB:	7 NO
	vCores: 4 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Windows 2012 R2| DB:	13 NO
	vCores: 16 | RAM: 24 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2100 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 3000 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2220 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1860 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 42 | RAM: 128 GB | Usable Performance Storage (800-1200 IOPs/TB): 2875.392 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2872.8 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 24 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2394 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 2160 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 80 GB | Usable Performance Storage (800-1200 IOPs/TB): 1860 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 80 GB | Usable Performance Storage (800-1200 IOPs/TB): 2936.832 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 24 | RAM: 80 GB | Usable Performance Storage (800-1200 IOPs/TB): 2220 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 128 GB | Usable Performance Storage (800-1200 IOPs/TB): 1810 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 24 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1810 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 32 | RAM: 128 GB | Usable Performance Storage (800-1200 IOPs/TB): 2880 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1440 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1688 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 12 | RAM: 24 GB | Usable Performance Storage (800-1200 IOPs/TB): 840 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 12 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: Windows 2012 R2| DB:	4 NO

	vCores: 8 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1380 GB | OS: RHEL 7.8| DB: PostgreSQL	2 NO
	vCores: 8 | RAM: 102 GB | Usable Performance Storage (800-1200 IOPs/TB): 41000 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 8 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Windows 2012 R2| DB:	7 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1836 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 1836 GB | OS: RHEL 7.8| DB: PostgreSQL	2 NO
	vCores: 8 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 120 GB | OS: CentOS| DB: MySQL CE	2 NO
	vCores: 32 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 100 GB | OS: CentOS| DB:	1 NO
	vCores: 24 | RAM: 36 GB | Usable Performance Storage (800-1200 IOPs/TB): 100 GB | OS: CentOS| DB:	1 NO
	vCores: 32 | RAM: 36 GB | Usable Performance Storage (800-1200 IOPs/TB): 100 GB | OS: CentOS| DB:	1 NO
	vCores: 24 | RAM: 125 GB | Usable Performance Storage (800-1200 IOPs/TB): 3120 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
	vCores: 4 | RAM: 8 GB | Usable Performance Storage (800-1200 IOPs/TB): 120 GB | OS: Windows 2012 R2| DB:	2 NO
	vCores: 8 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 240 GB | OS: Windows 2012 R2| DB:	2 NO
	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 3541.2 GB | OS: RHEL 7.8| DB: PostgreSQL	2 NO
	vCores: 16 | RAM: 4 GB | Usable Performance Storage (800-1200 IOPs/TB): 250 GB | OS: Windows 2012 R2| DB:	1 NO
	vCores: 16 | RAM: 4 GB | Usable Performance Storage (800-1200 IOPs/TB): 3792 GB | OS: RHEL 7.8| DB: PostgreSQL	1 NO
A.2	**Software Licenses**	**Unit**
OS	Windows Server	46 NO
	RHEL	26 NO
	CentOS	4 NO
DB	PostgreSQL CE	26 No.
	MySQL CE	2 No.
Monitoring Tool	Monitoring Tool for VMs, Ports & Firewall	101 NO
A.3	**Backup & Storage Solution**	**Unit**
Backup	Backup (Space+Software)	18 TB
Storage	Additional Backup Storage (for File Share)	240 TB
A.4	**Network & Connectivity Services**	**Unit**
Services	vLoad Balancer (1 Gbps Throughput)	24 NO
	Public IP's	25 NO
	Unmetered Internet Bandwidth at Datacenter Site	250 Mbps
A.5	**Security Services**	**Unit**
Services	vFirewall (1 Gbps Throughput)	4 NO
	vUTM (1 Gbps Throughput)	1 NO

	SIEM Tool	77 NO
	DDOS As a Service	1 NO
	Antivirus & HIPS	72 NO
	SSL Certificate (DV+OV)	1 NO
	Vulnerability Assesment test (Yearly Twice)	2 NO
	VPN (2 Factor Authentication)	15000 NO
A.6	**Managed Hosting Services**	**Unit**
Services	Operating System Management Services	72 NO
	Storage Management Services	1 NO
	Backup Management Services	72 NO
	DB Management Services	24 NO
	vFirewall & vUTM Management Services	5 NO
	vLoad Balancer Management Services	24 NO

4.4LR DR

Env.	Hosting Components	
A.1	**Softwares**	**Unit**
Monitoring Tool	Monitoring Tool	5 NO
A.2	**Storage Solution**	**Unit**
Storage	Near DR Storage	108 TB
	Far DR Storage	108 TB
A.3	**Network & Connectivity Services**	**Unit**
Services	Cross Connect + Port Termination	2 NO
	Unmetered Internet Bandwidth at Datacenter Site	100 Mbps
	Shared P2P Link from DC to DR	100 Mbps
	ILL for Far DR (For Redundancy)	100 Mbps
A.4	**Security Services**	**Unit**
Services	vFirewall (1 Gbps Throughput)	4 NO
	vUTM (1 Gbps Throughput)	1 NO
	DDOS As a Service	1 NO
A.5	**Managed Hosting Services**	**Unit**
Services	Storage Management Services	1 NO
	vFirewall & vUTM Management Services	5 NO
	DR Drill (Yearly Twice)	2 NO

The existing infrastructure is expected to increase by 1.5 times over the period of two years.

4.5 Requirement for proposed LR applications

Upcoming Applications	App	DB	Data Formats	Resource Requirement	CPU	RAM	HDD	OS	DB	File Storage (TB)	Services Required
SVAMITVA	1	1	Raw Data - Images, Orthorectified, Feature extraced - Shp Files, Database, GeoTiff, PDF file, Excel sheets	vCores: 16 | RAM: 16 GB | Usable Performance Storage (800-1200 IOPs/TB): 1000 GB | OS: Ubuntu 20.04 LTS| DB: My SQL (MariaDB 10.4.20	16	16	1000	Ubuntu 20.04 LTS	My SQL (MariaDB 10.4.20		Public IP,SSL,WebVPN,Apache 2.4.39,Open SLL 1.1.1c,PHP 7.3.8
				vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: Ubuntu 20.04 LTS| DB:	16	32	300	Ubuntu 20.04 LTS			
Scanning of Old Documents	2	2	Raw Data - Images, Database, PDF file	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :60	16	32	300	RHEL 7.8	Post gre SQL	60	
Digitsation of Cadastral Maps	2	2	Raw Data - Images, Drawing files, Feature extracted Shp files, Database, Excel, PDF file	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :1200	16	32	300	RHEL 7.8	Post gre SQL	1200	
EQJ Court	1	1	Database, PDF files	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :5	16	32	300	RHEL 7.8	Post gre SQL	5	

eMojani	2	2	Images,Drawing files, Database,PDF files, GIS data, Shp files	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :15	16	32	300	RHEL 7.8	Postgre SQL	15	
eChawadi	2	2	Database, PDF File	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :	16	32	300	RHEL 7.8	Postgre SQL		
ePeakPahani	2	2	Images, Database,PDF file	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :10	16	32	300	RHEL 7.8	Postgre SQL	10	
Website for Department	1	1	Images, Database,PDF file, Audio files	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :	16	32	300	RHEL 7.8	Postgre SQL		
Project Monitoring - Dashboard	1	1	Database, PDF file	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :	16	32	300	RHEL 7.8	Postgre SQL		

Service Portal	2	2	Database, PDF file	vCores: 16 | RAM: 32 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :	16	32	300	RHEL 7.8	Postgre SQL		
GIS Portal	2	2	Raw Data - Images,Orthorectified,Feature extraced,database,GeoTiff,PDF File, Excel file	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :800	16	64	300	RHEL 7.8	Postgre SQL	800	
Bhunaksha	2	2	Database,Feature extraced - Shp Files	vCores: 16 | RAM: 64 GB | Usable Performance Storage (800-1200 IOPs/TB): 300 GB | OS: RHEL 7.8| DB: PostgreSQL| File Storage :3	16	64	300	RHEL 7.8	Postgre SQL	3	
Total	**20**	**20**			**208**	**464**	**4600**			**2093**	

Note:

- The bidders should study the existing infrastructure and make necessary assumptions for designing the architecture for the department