Guidelines to the Government Departments for procuring Cloud Services

INDEX

Data Reference - https://www.meity.gov.in/

Compiled by – Ganesh Palve

Guidelines to the Government Departments for procuring Cloud Services from the Cloud Service Provider (CSP), Managed Service Provider (MSP) and Systems Integrator (SI)

(Ministry of Electronics and Information Technology)

1. Empanelment of Cloud Service Offerings

Ministry of Electronics & Information Technology (MeitY) has empanelled multiple CSPs for three different Cloud Deployment Models:

1. Public Cloud
2. Virtual Private Cloud
3. Government Community Cloud

The CSPs empanel their cloud services offerings through GeM. The empanelled cloud services will be published through a GI Cloud Services Directory for use by government departments or agencies at the Centre and States.

Following are the Cloud service offerings offered by the CSPs for a combination of the Deployment Models:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

2. General Requirements for all Cloud Deployment Model

The below mandatory requirements are applicable for all Cloud Deployment Models i.e. Public Cloud, Virtual Private Cloud and Government Community Cloud

1. 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 requirement of the Government Department) during any unanticipated spikes in the user load. The provisioning / de-provisioning SLAs may differ for the different Cloud Deployment Models.

2. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures

3. The respective Government Department shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

4. The respective Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

5. The respective Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.

6. The respective Government Department shall be provided access rights (including the underlying secure connection) to the user administration / portal of Cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service Providers.

7. CSP shall not provision any unmanaged VMs for the applications.

8. CSPs shall provide interoperability support with regards to available APIs, data portability etc. for the Government Department to utilize in case of change of Cloud Service Providers, migration back to in-house infrastructure, burst to a different Cloud Service Providers for a short duration or availing backup or DR services from a different service provider.

9. CSPs shall adhere to the ever-evolving guidelines as specified by CERT-In (http://www.certin.org.in/)

11. CSPs shall also adhere to the relevant audit requirements as defined in the application document or any new requirement as published by MeitY or STQC.

12. CSPs need to adhere to the guidelines and acts published by Government of India. No data should be shared to any third party without explicit approval by the User Department, unless legally required to do so by the courts of India. The empanelled Cloud services shall have to comply with the guidelines & standards as and when published by Govt. of India. CSPs shall be responsible for all costs associated with implementing, assessing, documenting, and maintaining the empanelment, any guidelines published by MeitY shall be followed by the CSPs. In case any misconduct is found, MeitY/ User Department reserves the right to take appropriate legal course of action including blacklisting of the CSP.

13. In case of any delay in publishing guidelines / standards by MeitY or identification of any critical gaps or deemed as required by MeitY during the period of empanelment, additional guidelines / standards may be published by MeitY from time to time that will be applicable for the empanelled Cloud Service Offerings of the Cloud Service Providers. The empanelled Cloud Service Offerings must comply with the additional guidelines / standards (applicable for the empanelled Cloud Service Offerings) as and when MeitY publishes such guidelines / standards, at no additional cost to retain the empanelment status. Cloud Service Providers shall be given sufficient time and notice period to comply with the additional guidelines / standards. Any downtime during such approved upgrades shall be considered as approved downtime for SLA calculations.

3.Detail Requirements for all Cloud Service Models

The below requirements shall be applicable on all the Cloud services offered from any of the Cloudservices model, i.e. Infrastructure as a Service, Platform as a Service, Software as a Service, offeredusing Public Cloud, Virtual Private Cloud and Government Community Cloud

a) Service Management and Provisioning Requirements

The CSPs shall ensure below mentioned requirements while provisioning the Cloud solution for the User Department are met.

1. Provisioning of virtual machines, storage and bandwidth dynamically (or on-demand) on aself-service mode or as requested.
2. Enable Service Provisioning via Application Programming Interface (API).

3. Secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]

4. Support the terms of service requirement of terminating the service at any time (on-demand).

5. Portal provisioned for the User Departments by the CSPs shall also contain the following information:

    a. Service Level Agreements (SLAs)

    b. Help Desk and Technical Support

    c. Resources (Technical Documentation, Articles/Tutorials, etc.

6. The CSPs shall carry out the capacity planning and do the Infrastructure sizing for the User Department to identify & provision, where necessary, the additional capacity to meet the usergrowth 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.

7. The CSPs shall ensure that the effective Remote Management features exist so that issues are addressed by the CSPs in a timely and effective manner.

8. Service Provisioning shall be available with two-factor / multi factor authentication via the SSL through a web browser.

b) Operational Management

1. The CSPs shall ensure that technology refresh cycles are conducted from time to time to meetthe performance requirements and SLAs. The management of network, storage, server, and virtualization layers, platforms as included by CSPs as part of their service offerings etc. shall be complete responsibility of CSPs during the technology refresh cycle.

2. The CSPs shall provide a secure, dual factor / multi-factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure.

3. The CSPs shall ensure that hardware is upgraded periodically without any financial impact tothe Government Department(s).

4. The applications / data hosted within the CSP environment shall be immediatelydeleted/destroyed and certify the VM and data destruction to the Government Department asper stipulations and shall ensure that the data cannot be forensically recovered.

5. CSPs shall ensure that patch management is performed from time to time or as & when required. CSPs shall alert the User Department in advance of any installation of patches via e-mail and cloud portal.

6. Patch management for OS security patches shall be responsibility of the CSP.

7. CSPs shall ensure that all OS images created within the Cloud platform are regularly patchedwith the latest security updates.

8. CSPs shall monitor availability of the servers, system software's and its network.

9. CSPs shall investigate outages, perform appropriate corrective action to restore the hardware, software, operating system, and related tools.

10. CSPs shall ensure that the software required by the User Department are provided with latestversion. However, if required by the User Department, the operating system and database maybe provisioned with not more than two version old (n-2, n being the latest version

c) Data Management

1. CSPs shall enforce security controls and policies to secure data from unauthorized access in amulti-tenant environment

2. CSPs shall provide tools and mechanisms to the Government Department or its appointed agency for defining its backup requirements & policy. The backup policy which is defined andimplemented shall be an automated process and backups should be taken on differentmediums.

3. The CSPs shall provide tools and mechanisms to the Government Department or its appointedagency 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.

4. CSPs shall be liable to transfer data back in-house or any other Cloud / physical environmentas required by the User Department, either on demand or in case of contract or order termination for any reason.

5. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.

6. CSPs shall ensure minimum 128-bit encryption is used for handling data at rest and in transit.

7. The CSPs shall be responsible for deleting or otherwise securing Government Department's Content/Data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered when the Government Department or CSP (with prior approval of the Government Department) scales down the services.

d) User/Admin Portal Requirements

The CSP shall be responsible to meet the below requirements:

Utilization Monitoring

a. Provide automatic monitoring of resource utilization and other events such as failure ofservice, degraded service, etc. via service dashboard or other electronic means.

b. Real time performance thresholds

c. Real time performance health checks

d. Real time performance monitoring & Alerts

e. Historical Performance Monitoring

f. Capacity Utilization statistics

g. Cloud Resource Usage including increase / decrease in resources used during auto-scale

Incident Management

h. Provide Incident Management and Ticketing via web-based portal (tools) for any incident occurrence during the operations.

i. CSPs shall follow and adhere to ITIL V3/V4 guidelines and process for the Incident management and Problem management.

j. CSPs shall provide a mechanism to carry out regular health check on Departmentprovisioned cloud infrastructure and facilitate download of the health check report as perthe frequency identified/set by the User Department.

k. For all Incidents / Issues with Severity 'Critical and High', the CSPs Incident Management Team shall be activated to provide resolution as per defined SLA's by the User Department and closure of the Incident. The teams shall be responsible to send an Incident Report on daily basis or as desired by User Department for all such Incidents toall the stake holders including designated officials by the department.

User Profile Management

l. Support maintenance of user profiles

m. CRUD Operations (CREATE, READ, UPDATE, DELETE)

e) Integration Requirements

Provide support to all Application Programming Interfaces (APIs) including REST API that CSP develops/provides.

f) LAN / WAN Requirements

1. The CSPs shall ensure that Local Area Network (LAN) does not impede data transmission.

2. Provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from CSP pool.

3. Ability to deploy VMs in multiple security zones as required for the project, defined by network isolation layers in the Customer's local network topology.

4. Provide access to Wide Area Network (WAN).

5. Provide private connectivity between a Government Department's network and Data Center Facilities.

6. 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.

7. Provide infrastructure that is IPv6 compliant.

8. CSPs shall support for providing secure connection to the Data Centre and Disaster RecoveryCentre (where applicable) from the Government Department Offices.

9. The Data Centre and Disaster Recovery Centre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity totake care of the needs of various types of user entities. Provision has to be made for segregationof access path among various user categories.

10. Support dedicated link to the offices of Government Departments to access the Data Centre and a separate internet link for other external stakeholders to get access to Government Department services.

11. CSPs shall have the capability to provide adequate bandwidth between Primary Data Centre and Disaster Recovery Centre for data replication.

g) Backup Services

1. The CSPs shall configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per thepolicy defined by MeitY or the Government Department.
2. The CSPs shall be responsible for file system and database backup and restore services.
3. The CSPs shall be responsible for back up of virtual machines, storage volumes, file systems, and databases within the CSP's own Cloud environment.
4. The CSPs shall be responsible for monitoring, reporting, notifications/alerts & incidentmanagement, backup storage, scheduling & retention, restoration, backup data protection, etc.
5. The backup solution shall support retention period of minimum 30 days or as desired by the User Department as per their needs.
6. The backup solution offered by CSPs shall support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc. Government Organization shouldbe able to recover individual files, complete folders, entire drive, or complete system to sourcemachine or any other machine available in network.
7. 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

h) Data Centre Facilities Requirements

1. The Data Centre facilities shall cater for the space, power, physical infrastructure (hardware).
2. The Data Centre facilities and the physical and virtual hardware should be located within India.
3. The space allocated for hosting the infrastructure in the Data Centre should be secure.
4. The Data Centre should be certified with the latest version of ISO 27001 (year 2017) and provide service assurance and effectiveness of Management.

5. The NOC and SOC facility must be within India for the Cloud Environments and the managedservices quality should be certified for ISO 20000-1:2018.
6. For any Government body / organization which shall avail Cloud services under this empanelment process, the CSPs shall be required to provide complete access of the IT Infrastructure to CERT-In. MeitY or any designated body selected by MeitY / User Department shall be able to carry out SOC and NOC operations for the MeitY empanelled services.
7. The Data Centre should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.
8. All the physical, environmental and security features, compliances and controls of the Data Centre facilities (as required under this application document) shall be enabled for the environment used for offering Cloud services.
9. Provide staff (technical and supervisory) in sufficient numbers to operate and manage the functioning of the DC & DR with desired service levels.
10. The Data Centre should comply with the Physical Security Standards as per ISO 27001:2017 standards.
11. CSPs shall be required to provide complete access of the Cloud Services to User Department or any designated body authorized by the User Department to carry out SOC and NOC operations.
12. The Applicant has to provide an undertaking on Data Centre service arrangements

i) Cloud Storage Service Requirements

1. The CSPs shall ensure that the cloud storage services are made available online, on-demand, and dynamically scalable up or down as per request from the end users (Government Department or Government Department's nominated agencies) with two-factor authentication via the SSL through a web browser.

2. The CSPs shall provide scalable, redundant and dynamic storage facility.

3. The CSPs shall provide users with the ability to add / remove storage with two-factor authentication via the SSL through Cloud management portal and manage storage capabilitiesremotely via the SSL VPN clients as against the public internet.

j) Disaster Recovery & Business Continuity Requirements

1. CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center of the Government Department and meet the RPO and RTO requirements.

    a. RPO should be less than or equal to 2 hours

    b. RTO shall be less than or equal to 4 hours

    c. Key transaction data shall have RPO of 15 minutes.

    However, the User Department may seek more stringent RTO, RPO, or any other disasterrecovery requirements as per their needs.

2. During the change from Primary DC to DR or vice-versa (regular planned changes), there should be minimal/no data loss depending on application requirements of the User Department.

3. There shall be asynchronous replication of data between Primary DC and DR and the CSP willbe responsible for sizing and providing the DC-DR replication link so as to meet RTO and RPOrequirements.

4. The DC & DR sites shall be separated by a minimum distance of 100 kilometers.

5. Replication Link sizing and provisioning shall be in scope of the CSP.

6. During normal operations, the Primary Cloud Data Centre shall 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 on demandbasis for a functional DR and minimum compute if required, as per the solution offered by theCSP or as desired by the User Department. The application environment shall be installed andready for use.

7. In the event of a site failover or switchover, DR site shall take over the active role, and all the requests

shall be routed through that site. Application data and application states shall be replicated between Data Centres so that when an outage occurs, failover to the surviving DataCentre can be accomplished within the specified RTO. The compute environment for the application shall be equivalent to DC during this period.

8. The installed application instance and the database shall be usable, and the same SLAs as DCshall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.

9. The security provisioned by CSP shall be for full infrastructure i.e. Cloud-DC and Cloud-DR.

10. The CSPs shall conduct DR drill once in every six months, of operation wherein the Primary DC shall be deactivated, and complete operations shall be carried out from the DR Site. However, during the change from DC to DR-Cloud or vice-versa (or regular planned changes),there should be no/minimal data loss depending on the application requirements of the userdepartment.

11. The CSPs shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSPs shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the period required for migrating to DR. The CSPs shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the User Department at least 15 working days before such drill.

12. RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions should be offered as part of the offering.

13. Any lag in data replication should be clearly visible in dashboard and its alerts should be sentto respective authorities.

14. The CSPs shall provide the solution document of DR to the User Department availing DR services.

15. The CSPs shall have proper escalation procedure and emergency response in case of failure/disaster at DC.

16. The CSPs shall demonstrate the DR site to run on hundred percent capacity for proving successful implementation of the DR site.

17. Automated switchover/failover facilities (during DC failure & DR Drills) to be provided and ensured by the CSP. The switchback mechanism shall also be automated process and no /minimal data loss depending upon application requirement of the User Department.

k) Security Requirements

1. The CSPs shall be responsible for provisioning, securing, monitoring and maintaining the hardware, network(s), and software that supports the infrastructure and present Virtual Machines (VMs) and IT resources to the Government Department.

2. The Data Centre Facility of the CSP shall at minimum implement the security toolset: Security& Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi FactorAuthentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDoS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

3. The CSPs shall ensure that they meet the ever-evolving security requirements as specified byCERT-In (http://www.cert-in.org.in/).

4. The CSPs shall ensure that they comply to Cloud Security ISO Standard ISO 27017:2015 and Privacy Standard ISO 27018:2019.

5. Meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP byMeitY as a mandatory standard.

6. MeitY and Government Department reserves the right to verify the security test results. In case of the Government Community Cloud, MeitY and Government Department reserves theright to verify the infrastructure.

7. Implement industry standard storage strategies and controls for securing data in the StorageArea Network so that clients are restricted to their allocated storage.

8. Ability to create non-production environments and segregate (in a different VLAN) non- production environments from the production environment such that the users of the environments are in separate networks.

9. Cloud Offerings should have built-in user-level controls and administrator logs for transparency and audit control.

10. Cloud Platform should be protected by fully-managed Intrusion detection system usingsignature, protocol, and anomaly-based inspection, thus providing network intrusion detection monitoring.

11. Cloud Platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.

12. Cloud Platform should provide Web Application Filter for OWASP Top 10 protection as a service that can be enabled for Government Departments that require such a service.

13. Access to Government Department provisioned servers on the Cloud should be through SSL VPN clients only as against the public internet.

14. CSPs shall allow audits of all administrator activities performed by Government Departmentand allow Government Department to download copies of these logs in CSV or any other desired format.

15. Maintain the security features described below, investigate incidents detected, undertake corrective action, and report to Government Department, as appropriate.

16. CSPs shall deploy and update commercial anti-malware tools (for systems using Microsoft operating systems), investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.

17. CSPs shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers.

18. CSPs shall ensure that password policies adhere to security requirements as defined by CERT-IN.

19. CSPs shall ensure that all GoI IT Security standards, policies, and reporting requirements aremet.

20. CSPs shall meet and comply with all GoI IT Security Policies and all applicable GoI standardsand guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

21. CSPs shall generally and substantially and in good faith follow GoI guidelines and CERT-In and MeitY Security guidance. Where there are no procedural guides, generally accepted industry best practices for IT security shall be used by the CSPs.

22. Information systems must be assessed whenever there is a significant change to the system's security posture.

23. MeitY or MeitY appointed 3rd party shall conduct regular independent third-party assessments of the CSP's security controls to determine the extent to which security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting security requirements and submit the results to MeitY and User Department.

24. In case CSP has industry standard certifications (assessed by a Third Party Auditor) that verify compliance against the security requirements of the application document, SLA & MSA, results, relevant reports, certifications may be provided with evidence along with the mappingof the industry standard certification controls against the application document requirements.However, if there are any requirements that do not fall under the industry standard certifications, the CSP shall get the Third Party Auditor to assess the conformance to the requirements.

25. MeitY reserves the right to perform Penetration Test. If MeitY exercises this right, the CSP shall allow MeitY's designated third party auditors to conduct activities to include control reviews that include but are not limited to operating system vulnerability scanning, web application scanning and database scanning of applicable systems that support the processing, transportation, storage, or security of Department's information. This includes the general support system infrastructure.

26. CSPs shall ensure that Identified gaps are tracked for mitigation in a Plan of Action document.

27. CSPs shall be responsible for mitigating all security risks found and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate riskvulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

28. CSPs shall provide access to MeitY or their designee acting as their agent when requested, in order to verify compliance with the requirements for an Information Technology security program. MeitY reserves the right to conduct on-site inspections. CSPs shall make appropriatepersonnel available for interviews and documentation during this review. If the documentation is considered proprietary or sensitive, these documents may be reviewed on- site under the CSP's supervision.

29. CSPs shall provide vulnerability scan reports from Web Application, Database, and OperatingSystem Scans or the services for the Government Department to run the vulnerability scan. The scan results (that fall under the scope of the CSP) shall be managed and recorded in Plansof Action and mitigated by the CSP.

30. All documents exclusively produced for the project are the property of the Government Department and cannot be reproduced or retained by the CSP. All appropriate project documentation will be given to Government Department during and at the end of this contractor at the time of termination of the contract. The CSP shall not release any project information without the written consent of the Government Department. Any request for information relating to the Project presented to the CSP must be submitted to the Government Departmentfor approval.

31. CSPs shall protect all Government Department data, equipment, etc. by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment shallonly be disclosed to empanelled-personnel from the User Department. CSPs shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to Government Department control, destroyed, or held until otherwise directed by the Government Department. CSPs shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

32. MeitY has the right to perform manual or automated audits, scans, reviews or other inspections of the CSP's IT environment being used to provide or facilitate services for the User Departments through a MeitY's designated third party auditor. CSPs shall be responsiblefor the following privacy and security

safeguards.

33. CSPs shall not publish or disclose in any manner, without MeitY's written consent, the detailsof any safeguards either designed or developed by the CSPs under the Agreement or otherwiseprovided by the GoI& Government Department.

34. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall allow MeitY logical and physical access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include but are not limited tothe following methods:

    i. Authenticated and unauthenticated operating system/network vulnerability scans

    ii. Authenticated and unauthenticated web application vulnerability scans

    iii. Authenticated and unauthenticated database application vulnerability scans

35. Automated scans shall be performed by MeitY's designated third party auditors using MeitY specified tools. If the CSP chooses to run its own automated scans or audits, results from thesescans may, at MeitY's discretion, be accepted in lieu of MeitY performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by MeitY. In addition,the results of CSP-conducted scans shall be provided in full to MeitY.

36. Submission to regular audits: CSPs shall submit documents as desired for regular audits commissioned by MeitY. The purpose of these audits shall not only be to ensure conformancewith the requirements stated in this application document, but also to ensure that theimplementation is executed in the best of ways to meet the requirements of MeitY. These audits may be conducted by MeitY or MeitY's designated third party auditors. CSP will cooperate fully with the auditor. MeitY will inform the CSP of the short-comings if any after the audit is completed and the CSP will respond appropriately and address the identified gaps.

37. For compliance to the government regulations, it is required that Cloud services offered shallbe hosted within India and data residency shall also be limited to the boundaries of India.

38. All data functions and processing shall be performed within the boundaries of India.

39. No data, whether in the form of backups or otherwise should be transmitted outside the boundaries and legal jurisdiction of India.

40. CSPs shall have capability / feature to define strong password policy and maintaining password complexity rules and shall also include the prohibition of changing of password/PINlengths and any authentication requirements.

41. CSPs shall also make sure that copy of customer data will be provided in the standard formatto

maintain portability.

42. CSPs shall ensure that all the policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and completeremoval of data.

l) Legal Compliance Requirements

The CSPs shall be liable to comply with all the legal requirements defined by MeitY.

1. IT Act 2000 (including 43A) and amendments thereof.
2. Meet the ever-evolving security requirements as specified by CERT-In (http://www.cert- in.org.in/).
3. Meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP byMeitY as a mandatory standard.
4. All services acquired under this application document including data will be guaranteed to reside in India only.
5. There shall not be any legal frameworks outside Indian Law applicable to the operation of theservice (and therefore the information contained within it).
6. A copy of the contract / MoU (excluding the commercials) between CSP & Government Department for the purpose of the project, aligned to the terms & conditions of the applicationdocument should be provided to MeitY, as and when requested by MeitY.
7. MeitY has initiated the process of identification of the standards, develop the necessary specifications, frameworks and guidelines including the guidelines for empanelment of CloudService Offerings. The guidelines may also include continuous monitoring of the shared systems that can be leveraged by Government to both reduce their security compliance burden and provide them highly effective security services.
8. The empanelled Cloud services shall have to comply with the guidelines & standards as and when such guidelines / standards are published by MeitY within the timeframe given by MeitY.
9. CSPs shall be prepared to submit the necessary artifacts and independent verification withinthe timeframe determined by MeitY once the guidelines & standards are published by MeitY.
10. CSPs shall be responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the registration.
11. The cost of meeting all requirements, maintaining empanelment of it's Cloud Service Offering shall be the responsibility of CSP.
12. If the CSP fails to meet the guidelines & standards as set by GoI within the timeframe set by MeitY, the Government Department reserves the right to terminate the contract and request to move to a

different CSP that meets the mandatory guidelines & standards at no additional

cost to Government Department. The Exit Management provisions shall come into effect insuch a scenario.

13. CSPs shall be responsible for the following privacy and security safeguards:

    a. CSPs shall not publish or disclose in any manner, without the Government Department's written consent, the details of any safeguards either designed or developed by the CSP under the agreement or otherwise provided by the GovernmentDepartment or Government of India.

    b. CSPs shall adhere to the privacy safeguards as laid down by the MeitY and Government Department.

    c. To the extent required to carry out a program of inspection to safeguard against threats and hazards to security, integrity and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the MeitY or its nominated agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.

    d. If new or unanticipated threats or hazards are discovered by either MeitY or Government Department, Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attentionof CERT-In and the other party.

    e. CSPs need to adhere to the guidelines and acts published by Government of India. Nodata should be shared to any third party without explicit approval by the User Department, unless legally required to do so by court of law in India.

14. The empanelled Cloud services shall have to comply with the guidelines & standards as and when published by Govt. of India. CSPs shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment and any guidelinespublished by MeitY shall be followed by the CSPs.

15. In case any misconduct is found, MeitY / User Department reserves the right to take appropriate legal course of action including blacklisting of the CSP.

m) Management Reporting Requirements

The CSPs shall ensure deliverables listed below should be accessible via online interface not laterthan 10 days after the end of the calendar month and available for up to one year after creation. The information shall be available in format approved by MeitY / User Department. The CSPs shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between the Government Department and the CSP. CSPs shall provide regular monthly reports to MeitY. In addition to this, MeitY reserves the right to seek any additional reports based on specific issues / concerns with respect to provisioning or availing Cloud services.

Cloud Service Providers shall also provision real time dashboard for monitoring and reportingpurposes for MeitY.

1. Service Level Management

    a. Service Level Management Reports (as per the service levels agreed in the Service Level Agreement between the Government Department and the CSP).

    b. Service Availability at the VM & Service Availability at the Storage Level (Measured as TotalUptime Hours / Total Hours within the Month) displayed as a percentage of availability upto one-tenth of a percent (e.g. 99.5%).

    c. Text description of major outages (including description of root-cause and fix) resulting ingreater than 1-hour of unscheduled downtime within a month.

2. Network and Security Administration (including security breaches with classification, actiontaken by the CSP and current status) related reports.

3. Help Desk / Trouble Tickets raised by the MeitY and / or Government Department.

4. Number of Help Desk/customer service requests received.

5. Number of Trouble Tickets Opened.

6. Number of trouble tickets closed.

7. Average mean time to respond to Trouble Tickets (time between trouble ticket opened and thefirst contact with customer).

8. Average mean time to resolve trouble ticket.

9. Monthly utilization (including peak and non-peak volumetric details) of the Service Offeringsfor the respective Government Department.

10. Centralized Monitoring & Management and Reporting with:

a. Alerts on event threshold and policy-based actions upon deviations.

b. Internet & Intranet Data Transfer.

c. Virtual Instances (vCPU, vMemory, Storage and Network Port) configuration and utilization.

d. Storage Volume (Read/Write and IOPS)

e. Load balancer

f. Database Monitoring

g. Reports on non-conformance and escalation for privileged access by unpaneled roles/ identities.

11. Government / User Departments shall have ten (10) business days to review, accept or rejectall deliverables. Any comments made by the Government Department shall be addressed anda revised deliverable submitted within five (5) business days after the receipt of the comments/rejection, unless a further time extension for incorporating the comments isapproved by Government Department.

12. The CSPs shall be responsible for third party audits certification (at the cost of CSP) every sixmonths indicating the conformance to the requirements detailed in this application document of the empanelment of Cloud services which are being used by the Government Department. In case the empanelled Cloud services are not deployed for any Government Department, a self-certification every six months indicating the conformance to the requirements detailed in this application document, SLA & MSA of the environments & Cloud Service Offeringsempanelled should be provided to MeitY.

13. CSPs shall provide regular monthly reports having at least the following information about the User Department procuring the Cloud services, Name of the Cloud services, Cloud Deployment Model (s) selected, Cloud Service Model (s) selected, Month & Year of Award of Work Order) to MeitY as per the report template shared by MeitY.

n) Service Level Agreement Management

1. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assureduptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels.

2. Service Availability (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%).

3. Within a month of a major outage occurrence resulting in greater than 1-hour of unscheduled downtime. Describe the outage including description of root-cause and fix.

4. Service provisioning and de-provisioning times (scale up and down) in near real- time shouldbe as per the SLA requirement of the Government Department. The provisioning / de- provisioning SLAs may differ for the different Cloud Deployment Models.

5. Helpdesk and Technical support services to include system maintenance windows.

6. CSPs shall implement the monitoring system including any additional tools required for measuring and monitoring each of the Service Levels as per the SLA between the GovernmentDepartment and the CSP.

4. Responsibility of CSP & Govt Department when Direct Procurement of Cloud Services from CSP

a) Responsibility of Government Departments:

- Government Department should have in place an Implementing Agency/Internal IT Team or expertise that is responsible for managing Cloud resources

b) Responsibilities of CSP:

- Offer services in accordance with the Cloud Service Model opted by the User Department
- Offer the User Department with the elements such as facilities, data centres, network interfaces, processing, hypervisors, storage, and other fundamental
- computing resources where the department is able to deploy and run Cloud Service Model.
- CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc.
- Ensure successful network connectivity is established between the User Department location(s) and Cloud DC-DR site
- Ensure the appropriate security controls for physical and logical security are in place at Cloud DC and DR
- Ensure data is successfully replicated between the Cloud DC and Cloud DR and as per the required RPO specified by the User Department
- Ensure successful replication link is established between Cloud DC and DR site

5.Cloud Security

Cloud Security Unlike traditional IT systems, cloud computing refers to on demand access of infrastructure and services. Herein the CSP is responsible for making available the cloud platform and services portfolio which is configured and managed by the MSP for the client/user. Depending on the skillset, the user may themselves configure and manage the cloud platform in which case an MSP may not be required.

Cloud computing allows the Government Departments to access the software, hardware, and other necessary infrastructure required to run its daily operations. Furthermore, the cloud ensures easier data management and system security. Instead of controlling every aspect of data security control on-site, the Department can easily outsource the data security needs to a prominent and reputable Managed Service Provider.

On-premises infrastructure may be more exposed to small slip-ups and errors that can be prone to cyber-attacks. Furthermore, most cloud developers are more experienced with advanced security and data governance models. This means that the Departments will be able to plan appropriate strategies to ensure real time risk mitigation. An important reason for the reluctance to move more data into the cloud are the concerns around security. A comparison between On-premise and cloud setups with security at the centre has been highlighted below.

	On-premise/ Co-located DC	Cloud
Technical Expertise	Government Department's own team or an IT Managed Service Provider	Cloud Managed Service Provider
Security Technology Upgrade	Less frequent	More frequent
Physical DC Security	Government Department/ Co-location DC Provider	Cloud Service Provider
IT Infrastructure Security	Government Department/Co-location DC Provider	Cloud Service Provider
Vulnerability/ Security Patching	Depends on support levels and technical expertise of in-house team	More frequent and up to date
Certifications & Compliances	Government Department	Cloud Service Provider
Resiliency (Downtime)	Less Resilient with varying commitments on downtime	More Resilient and committed uptime and availability SLAs