CSP-01- 07

Audit Report of Cloud Service Provider

December 2016
(**CSP-01-07), Issue-1**

STQC Directorate,
Ministry of Electronics & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003.

Title: Audit Report of Cloud Service Provider

Purpose: Purpose of this Audit Report format is to provide information for audit decision (or otherwise) in a uniform presentation. This makes easy to correlate with the audit criteria specified in the scheme.

Responsibility: Leader of the assessment team (Lead Asscessor) is responsible to prepare this report. He shall collect all the necessary information from his team members to complete this report. The reference of the objective evidence can be attached in the Annexure. Under the column Auditor Comment explicit statement regarding compliance (C), non-compliance (NC), partially compliance (PC) shall be stated.

Conformance to General Requirements of Government community cloud, private cloud and virtual private cloud.

S. No.	Nature of the Requirement	Auditor's Comment
1.	Shall be in accordance with the definitions of various terms and conditions in the Service Level Agreement and Master Services Agreement) (reference of the process).	
2.	There should be a process for at least 30% headroom (at an overall level in the compute & Storage capacity offered) available for near real time provisioning during any unanticipated spikes in the user load(reference of the process).	
3.	Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures (reference of the process).	
4.	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 (reference of the process).	
5.	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	

	(reference of the process).	
6.	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 (reference of the process).	
7.	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 provider(reference of the process).	
8.	CSP shall not provision any unmanaged VMs for the applications (reference of the process).	
9.	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 provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider (reference of the process).	
10.	Should adhere to the ever evolving guidelines as specified by CERT-In (http://www.certin.org.in/) (reference of the process).	
11.	Should adhere to the relevant standards published (or to be published) by MeitY or any standards body setup / recognized by Government of India and notified to the CSP by MeitY as a mandatory standard (reference of the process).	
12.	CSP shall also adhere to the relevant audit requirements as defined in the RFP (reference of the process).	
13.	MeitY has initiated the process of identification of the Standards; develop the necessary specifications, frameworks and guidelines with the help of a Cloud Management Office (CMO). The provisionally accredited cloud service offerings will have the option to comply with the full-fledged guidelines & standards as and when the such guidelines / standards are published by MeitY to get the full accreditation within the timeframe given by MeitY. CSP is responsible for all costs associated with implementing, assessing, documenting and maintaining the accreditation (reference of the process).	
14.	In case of any delay in publishing full-fledged guidelines / standards by CMO or identification of any critical gaps or deemed as required by MeitY during the period of provisional accreditation, additional guidelines / standards may be published by MeitY from time to time that will be applicable for the Provisionally Accredited Cloud	

	Service Offerings. Provisionally accredited cloud service offerings must comply with the additional guidelines / standards (applicable for the Provisionally Accredited Cloud Service Offerings) as and when such guidelines / standards are published by MeitY at no additional cost to retain the provisional accreditation status. Private Service Providers will be given sufficient time and notice period to comply with the additional guidelines / standards. Any downtime during such approved upgrades will be considered as approved downtime for SLA calculations (reference of the process).	
15.	Government Department has the option to extend the Provisional Accreditation duration on expiry, to avail the services of the CSP for continuation of the services without the need to go for a separate accreditation process. The duration of extension will be decided by Government Department and will be up to a maximum of one year. The decision on the extension will be taken exclusively by Government Department keeping in consideration (reference of the process).	
	a) satisfactory performance of the Agency	
	b) time constraints or other serious impediments in initiation / completion of full-fledged accreditation process	
	c) technological reasons d) Where circumstances inescapably require taking recourse to this option.	

Service Management and Provisioning Requirements

The below mandatory requirements are applicable for all cloud deployment models. Service Management and Provisioning requirements address the technical requirements for supporting the provisioning and service management of the Cloud Service Offerings proposed to be accredited. Service provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.

Service Provisioning		
S. No.	**Nature of the Requirement**	**Compliance Statement by auditor**

1.	Provide the ability to provision virtual machines, storage and bandwidth dynamically (or on-demand), on a self-service mode or as requested (reference of the process).	
2.	Enable Service Provisioning via online portal/interface (tools) (reference of the process).	
3.	Enable Service Provisioning via Application Programming Interface (API) (reference of the process).	
4.	Secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)] (reference of the process).	
5.	Support the terms of service requirement of terminating the service at any time (on demand) (reference of the process).	
6.	Provide a webpage and associated Uniform Resource Locator (URL) that describes the following: (reference of the process). a. Service Level Agreements (SLAs)	
	b. Help Desk and Technical Support	
	c.Resources(Documentation, Articles/Tutorials, etc)	
7.	Make the Management Reports described in RFP accessible via online interface. These reports shall be available for one year after being created (reference of the process).	
8.	The CSP is expected to 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 o f the solution. There should not be any constraints on the services (reference of the process).	
9.	The CSP shall ensure that effective Remote Management features exist so that issues can be addressed by the Government Department in a timely and effective manner (reference of the process).	
10.	Service Provisioning shall be available via the SSL VPN clients only as against the public internet (reference of the process).	
Service Level Agreement Management		
1.	Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels (reference of the process).	
2.	Document and adhere to the SLAs to include: (reference of the process).	

	a. 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%)	
	b. 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.	
	c. Service provisioning and de-provisioning times (scale up and down) in near real- time	
3.	Helpdesk and Technical support services to include system maintenance windows (reference of the process).	
4.	CSP 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 Government Department and the CSP (reference of the process).	
Operational Management		
1.	Manage the network, storage, server and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs (reference of the process).	
2.	Provide a secure, dual factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure (reference of the process).	
3.	Upgrade and periodically replace hardware without financial impact to the Government Department. All the data within it shall be immediately deleted/destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered (reference of the process).	
4.	Perform patch management appropriate to the scope of their control (reference of the process)	
	a. Alerts on the upcoming patches via email and management portal, and ability to defer or reject patches before they are applied in the next patch cycle	
	b. Patch approved VMs on the next available patch management change window;	

	c. Application of automated OS security patches, unless deferred or rejected by DeitY	
	d. Send regular approval reminders to MeitY and the Government Department designated email address five (5) days prior to patch cut-off dates	
5.	OS level vulnerability management – all OS images created within the cloud platform are regularly patched with the latest security updates (reference of the process).	
6.	Provide the artifacts, security policies and procedures demonstrating its compliance with the Security Assessment and Authorization requirements as described in Security Requirements in RFP (reference of the process).	
7.	Monitor availability of the servers, CSP -supplied operating system & system software, and CSP's network (reference of the process).	
8.	The CSP is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the CSP (reference of the process).	
9.	Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools (reference of the process).	
10.	CSP should manage CSP provisioned infrastructure including VMs as per the ITIL standards (reference of the process).	
11.	Comply with technology refresh requirements as required by the MeitY to ensure security requirements and service level agreements (SLA) are met (reference of the process).	
12.	Software within the CSP's scope will never be more than two versions behind unless deferred or rejected by DeitY (reference of the process).	
Data Management		
1.	Manage data isolation in a multi-tenant environment (reference of the process).	
2.	The CSP should provide tools and mechanism to the Government Department or its appointed agency for defining their backup requirements & policy (reference of the process).	
3.	The CSP should provide tools and mechanism to the Government 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, images, system state, databases and enterprise applications in an encrypted	

	manner as per the defined policy (reference of the process).	
4.	Transfer data back in-house either on demand or in case of contract or order termination for any reason (reference of the process).	
5.	Manage data remanence throughout the data life cycle (reference of the process).	
6.	Provide and implement security mechanisms for handling data at rest and in transit (reference of the process).	
7.	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 (reference of the process).	
8.	When the Government Department or CSP (with prior approval of the Government Department) scales down the infrastructure services, CSP is 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 (reference of the process).	

User/Admin Portal Requirements

The below mandatory requirements are applicable for all cloud deployment models

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	Utilization Monitoring (reference of the process)	
	a. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.	
	b. Real time performance thresholds	
	c. Real time performance health checks f. Capacity Utilization statistics	
	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	
2.	Trouble Management (reference of the process).	
	a. Provide Trouble Ticketing via online portal/interface (tools).	
	b. Provide Trouble Ticketing via API.	
3.	User Profile Management (reference of the process)	
	a. Support maintenance of user profiles and present the user	

	with his/her profile at the time of login	

Integration Requirements

The below mandatory requirements are applicable for all cloud deployment models.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	Local Area Network (LAN) shall not impede data transmission (reference of the process).	
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 (reference of the process).	
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 (reference of the process).	
4.	Provide access to Wide Area Network (WAN) (reference of the process).	
5.	Provide private connectivity between a Government Department's network and Data Center Facilities (reference of the process).	
6.	IP Addressing: (reference of the process)	
	a. Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).	
	b. Provide IP address and IP port assignment on external network interfaces.	
	c. Provide dedicated virtual private network (VPN) connectivity.	
	d. Allow mapping IP addresses to domains owned by the Government Department, allowing websites or other applications operating in the cloud to be viewed externally as Government URLs and services.	
7.	Provide infrastructure that is IPv6 compliant (reference of the process).	
8.	CSP shall support for providing the secure connection to the Data Center and Disaster Recovery Center (where applicable) from the Government Department Offices (reference of the process).	
9.	The data center and disaster recovery centre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories	

	(reference of the process).	
10.	Support dedicated link to the offices of the Government Department to access the data center and a separate internet link for the other external stakeholders to get access to Government Department services (reference of the process).	
11.	CSP shall have the capability to provide adequate bandwidth between Primary Data Center and Disaster Recovery Center for data replication purpose (reference of the process).	
12.	Support network level redundancy through MPLS lines from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc. These two network service providers 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 (reference of the process).	

Data Center Facilities Requirements

The below mandatory requirements are applicable for all cloud deployment models.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	The data center facilities shall cater for the space, power, physical infrastructure (hardware) (reference of the process).	
2.	The data center facilities and the physical and virtual hardware should be located within India (reference of the process).	
3.	The space allocated for hosting the infrastructure in the Data Center should be secured and exclusively earmarked (reference of the process).	
4.	The Data Center should be certified for the latest version of ISO 27001 (year 2013) and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards (reference of the process).	
5.	The NOC offered for the Data Center Facilities must be within India and the managed services quality should be certified for ISO 20000:1 (reference of the process).	
6.	The Data Center 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 (reference of the process).	
7.	All the physical, environmental and security features, compliances and controls of the Data Center facilities	

	shall be enabled for the environment used for offering cloud services (reference of the process).	
8.	Provide staff, technical and supervisory, in sufficient numbers to operate and manage the functioning of the DC & DRC with desired service levels (reference of the process).	
9.	Physical Security Standards as per the latest version of ISO 27001 (year 2013) standards (reference of the process).	
10.	Facility shall be certified (either with respect to Tier Standards or Physical Security Standards) by a Third Party at regular intervals indicating the conformance to the Tier III standards (reference of the process).	

Cloud Storage Service Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) via SSL VPN clients only as against the public internet through a web browser.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	Service shall provide scalable, redundant, dynamic storage (reference of the process).	
2.	Service shall provide users with the ability to procure and use storage capabilities remotely via the SSL VPN clients only as against the public internet (reference of the process).	
3.	Service shall provide storage capabilities on-demand, dynamically scalable per request and via the SSL VPN clients only as against the public internet (reference of the process).	
4.	Storage Space: Online, on-demand virtual storage supporting a single storage sizes of up to 5GB (reference of the process).	
5.	Data Transfer Bandwidth: Bandwidth utilized to transfer files/objects in/out of the providers infrastructure supporting a minimum of 100GB of data transferred (in and out) via the network (reference of the process).	
6.	There shall not be any additional costs associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for Government Department (reference of the process).	

Virtual Machine Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) via SSL VPN clients only as against the public internet through a web browser.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines (reference of the process).	
2.	Service shall allow Government Department authorized users to procure and provision computing services or virtual machine instances online via the SSL VPN clients only as against the public internet (reference of the process).	
3.	Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet (reference of the process).	
4.	Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into a MeitY approved image format (reference of the process).	
5.	Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the SSL VPN clients only as against the public internet (reference of the process).	
6.	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 Government 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 the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered (reference of the process).	
7.	CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions (reference of the process).	
8.	Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network (reference of the process).	
9.	CPU (Central Processing Unit) - CPU options shall be provided as follows: (reference of the process)	
	a. A minimum equivalent CPU processor speed of 2.4GHz shall be provided.	

	b. The CPU shall support 64-bit operations	
10.	Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform (reference of the process).	
11.	Provide hardware based load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers (reference of the process).	
12.	Support Clustering (reference of the process).	
13.	Operating System (OS) (reference of the process).	
	a. Service shall support one or more of the major OS such as Windows, LINUX.	
	b. Management of the OS processes and log files including security logs retained in guest VMs;	
	c. Provide anti-virus protection;	
	d. Provide OS level security as per CSP standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation;	
14.	Persistence (reference of the process).	
	a. Persistent Bundled Storage is retained when the virtual machine instance is stopped or	
	b. Non-Persistence – Non-Persistence Bundled Storage is released when the virtual instance is stopped. If quoting Non-Persistence VM, the CSP shall provide VM Block storage	
15.	RAM (Random Access Memory): Physical memory (RAM) reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM. Memory (RAM) requirement should be different for different type of servers such as web servers and database servers (reference of the process).	
16.	Disk Space options allocated for all virtual machines and file data supporting a minimum of 40GB bundled storage (reference of the process).	
17.	Virtual Machine Block Storage Service Requirements (reference of the process)	
	a. Service shall provide scalable, redundant, dynamic Web-based storage	
	b. Service shall provide users with the ability to procure and provision block storage capabilities for cloud virtual machines remotely via the SSL VPN clients only as against the public internet.	
	c. Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances.	

	d. Block Storage – Once mounted, the block storage should appear to the virtual machine like any other disk	
	e. storage Space: Online, on-demand storage volumes of arbitrary size ranging from 1 GB to at least 1 TB	
	f. Input/Output (I/O) Requests: Input/Output requests on block storage	
18.	Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the Department's application (reference of the process).	
19.	Government Department retains the right to request full copies of these virtual machines at any time (reference of the process).	
20.	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 (reference of the process).	
21.	Support a secure administration interface - such as SSL/TLS or SSH - for the Government Department designated personnel to remotely administer their virtual instance (reference of the process).	
22.	Provide the capability to dynamically allocate virtual machines based on load, with no service interruption (reference of the process).	
23.	Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing (reference of the process).	
24.	Provide capability to perform live migrations (ability to move running VM's) from one host to another (reference of the process).	
25.	Cloud provider should offer fine-grained access controls including role based access control, use of SSL certificates, or authentication with a multi-factor authentication (reference of the process).	
26.	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 (reference of the process).	
27.	Government Department should be permitted to bring and upload additional properly licensed non-operating system software for operation in cloud as required for the Government Department solution for use within the Services by installing it directly on a VM (reference of the process).	
28.	RAM or CPU of virtual machine should scale automatically whenever there is spike in load to deliver application availability even during spike in load (reference of the process).	

29.	Provide facility to configure virtual machine of required vCPU, RAM and Disk (reference of the process).	
30.	Provide facility to use different types of disk like SAS, SSD based on type of application (reference of the process).	

Disaster Recovery & Business Continuity Requirements

S. No.	Nature of the Requirement	Compliance Statement
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. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements(reference of the process).	
2.	The Primary DC (of the Government Department) and the DRC should be in different seismic zones (reference of the process).	
3.	During normal operations, the Primary Data Center (of the Government Department) 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 but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site (reference of the process).	
4.	In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. 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. This is the period during which the Compute environment for the application	

	shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall 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. 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. The CSP shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from Page 32 of 81the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss (reference of the process).	
5.	The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The 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 migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill (reference of the process).	
6.	The CSP should offer dashboard to monitor RPO and RTO of each application and database(reference of the process).	
7.	The CSP should offer switchover and switchback of individual applications instead of entire system(reference of the process).	
8.	Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities(reference of the process).	

Security Requirements

The below mandatory requirements are applicable for all cloud deployment models.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	CSP is responsible for provisioning, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present Virtual Machines (VMs) and IT resources to the Government Department. On its part, the Government Department is responsible for the security of the "guest" Operating System (OS) and any additional software, up to and including the applications running on the guest OS (reference of the process).	

2.	In case, the CSP provides some of the System Software as a Service for the project, CSP is responsible for securing, monitoring, and maintaining the System and any supporting software. Government Department is responsible for securing and maintaining the Government Department application (reference of the process).	
3.	The Data Center Facility shall at a minimum implement the security toolset: Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Single Signon, UTM, One Time Passwords, Multi Factor Authentication, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Web Application Filter for OWASP Top 10 protection, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting) (reference of the process).	
4.	Meet the ever evolving security requirements as specified by CERT-In (http://www.certin.org.in/) (reference of the process).	
5.	Meet any security requirements published (or to be published) by DeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DeitY as a mandatory standard (reference of the process).	
6.	DeitY and Government Department reserves the right to verify the security test results (reference of the process)	
	a. In case of the Government Community Cloud, DeitY and Government Department reserves the right to verify the infrastructure.	
7.	Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage (reference of the process).	
8.	Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer (reference of the process).	
9.	Ability to create non-production environments and segregate (in a different VLAN) nonproduction environments from the production environment such that the users of the environments are in separate networks (reference of the process).	
10.	Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control (reference of the process).	
11.	Cloud Platform should be protected by fully-managed Intrusion detection system using signature, protocol, and	

	anomaly based inspection thus providing network intrusion detection monitoring (reference of the process).	
12.	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 (reference of the process).	
13.	Cloud platform should provide Web Application Filter for OWASP Top 10 protection (reference of the process).	
14.	Access to Government Department provisioned servers on the cloud should be through SSL VPN clients only as against the public internet (reference of the process).	
15.	Provision of private network ports to be connected to Government Department network for additional secure connectivity between Government Department network and the cloud through support for MPLS, Fiber, P2P links (reference of the process).	
16.	Virtual Machines should not have console access (reference of the process).	
17.	Virtual Machines should not have console access (reference of the process).	
18.	Maintain the security features described below, investigate incidents detected, undertake corrective action, and report to Government Department, as appropriate (reference of the process).	
19.	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 (reference of the process).	
20.	Shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers (reference of the process).	
21.	CSP should enforce password policies (complex password, change password in some days etc) (reference of the process).	
22.	Shall be contractually subject to all GoI IT Security standards, policies, and reporting requirements. The CSP shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology (reference of the process).	
23.	Shall generally and substantially and in good faith follow GoI guidelines and CERT-In and DeitY Security guidance. Where there are no procedural guides, use generally accepted industry best practices for IT security (reference of the process).	

24.	Information systems must be assessed whenever there is a significant change to the system's security posture (reference of the process).	
25.	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 DeitY and Government Department (reference of the process).	
26.	Provide an independent Security Assessment/Risk Assessment (reference of the process).	
27.	DeitY reserves the right to perform Penetration Test. If the DeitY exercises this right, the CSP shall allow DeitY'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 (reference of the process).	
28.	Identified gaps shall be tracked for mitigation in a Plan of Action document (reference of the process).	
29.	CSP is responsible for mitigating all security risks found and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities (reference of the process).	
30.	Shall provide access to the DeitY or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. DeitY reserves the right to conduct on-site inspections. CSP shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the CSP's supervision (reference of the process).	
31.	Shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans. Scan results shall be managed and mitigated in Plans of Action (reference of the process).	
32.	All documents 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 contract or at the time of termination of the contract. The CSP shall not release any 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 Department for approval (reference of the process).	
33.	CSP shall protect all Government Department data, equipment, etc., by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment will only be disclosed to authorized-personnel. The CSP 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. The CSP shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material (reference of the process).	
34.	DeitY 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 Government Department through a third party auditor appointed or authorized by DeitY. CSP shall be responsible for the following privacy and security safeguards: (reference of the process)	
	a. CSP shall not publish or disclose in any manner, without the MeitY's written consent, the details of any safeguards either designed or developed by the CSP under the Agreement or otherwise provided by the GoI & Government Department.	
	b. 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 afford the DeitY 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 to, the 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 can be performed by MeitY or agents acting on behalf of the MeitY, using MeitY specified tools. If the CSP chooses to run its own automated scans or audits, results from these scans may, at the MeitY's discretion, be accepted in lieu of DeitY performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the MeitY. In addition, the results of CSP-conducted scans shall be provided, in full, to the MeitY (reference of the process).	
36.	Submission to regular audits: CSP will submit to regular audits commissioned by MeitY. The purpose of these audits will not only be to ensure conformance with the requirements stated in RFP, but also to ensure that the implementation is executed in the best of ways to meet the requirements of MeitY. These audits may be conducted by MeitY or any 3rd party auditor appointed by MeitY. 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 (reference of the process).	

Legal Compliance Requirements

The below mandatory requirements are applicable for all cloud deployment models.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	IT Act 2000 (including 43A) and amendments thereof (reference of the process).	
2.	Meet the ever evolving security requirements as specified by CERT-In (http://www.certin.org.in/) (reference of the process).	
3.	Meet any security requirements published (or to be published) by DeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DeitY as a mandatory standard (reference of the process).	
4.	All services acquired under RFP including data will be guaranteed to reside in India (reference of the process).	
5.	There shall not be any legal frameworks outside Indian Law applicable to the operation of the service (and therefore the information contained within it) (reference of the process).	

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 RFP, should be provided to MeitY (reference of the process).	
7.	MeitY has initiated the process of identification of the Standards, develop the necessary specifications, frameworks and guidelines including the guidelines for full-fledged accreditation of cloud service offerings with the help of a Cloud Management Office (CMO). 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 (reference of the process).	
	a. The provisionally accredited cloud service offerings will have the option to comply with the full-fledged guidelines & standards as and when the such guidelines / standards are published by MeitY to get the full accreditation within the timeframe given by MeitY	
	b. CSPs should be prepared to submit the necessary artifacts and the independent verification within the timeframe determined by MeitY once the guidelines & standards are published by MeitY.	
	c. CSP is responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the accreditation.	
	d. The cost of meeting all requirements, getting accredited and maintaining accreditation is the responsibility of CSP.	
	e. I f 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 in such a scenario.	
8.	CSP shall be responsible for the following privacy and security safeguards: (reference of the process)	
	a. CSP 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 Government Department or Government of India.	
	b. CSP 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 the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP	

	shall afford the DeitY 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 the 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 attention of CERT-In and the other party.	

Management Reporting Requirements

The below mandatory requirements are applicable for all cloud deployment models.

Deliverables listed below should be accessible via online interface not later than 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. The CSP shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between the Government Department and the CSP.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	Service Level Management (reference of the process)	
	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 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%)	
	c. Text description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month	
2.	Network and Security Administration (including security breaches with classification, action taken by the CSP and current status) related reports (reference of the process).	
3.	Help Desk / Trouble Tickets raised by the MeitY and / or Government Department (reference of the process)	
	a. Number of Help Desk/customer service requests received.	
	b. Number of Trouble Tickets Opened	
	c. Number of trouble tickets closed	
	d. Average mean time to respond to Trouble Tickets (time between trouble ticket opened and the first contact with customer)	

	e. Average mean time to resolve trouble ticket	
4.	Monthly utilization (including peak and non-peak volumetric details) of the Service Offerings for the respective Government Department (reference of the process).	
5.	Centralized Monitoring & Management and Reporting with: (reference of the process)	
	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. Application Services	
	g. Database Monitoring	
	h. Reports on non-conformance and escalation for privileged access by unauthorized roles/ identities	
6.	Government Department will have ten (10) business days, to review, accept or reject all deliverables. Any comments made by the Government Department shall be addressed and a revised deliverable submitted within five (5) business days after the receipt of the Comments/rejection, unless a further time extension for incorporating the comments is approved by Government Department (reference of the process).	
7.	Third Party Audit Certification (at the cost of CSP) every six months indicating the conformance to the requirements detailed in RFP of the accredited cloud service offerings which are being used by the Government Department. In case the accredited cloud service offerings are not deployed for any Government Department, a self certification every six months indicating the conformance to the requirements detailed in this RFP, SLA & MSA of the environments & cloud service offerings accredited should be provided to DeitY (reference of the process).	
8.	Any other reports as deemed required by MeitY from time-to-time (reference of the process).	

Exit Management and Transition Requirements

The below mandatory requirements are applicable for all cloud deployment models.

S. No.	Nature of the Requirement	Compliance Statement by auditor
1.	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 the Government Department. It is the prime responsibility of CSP to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded .Further, CSP is also responsible for all activities required to train and transfer t he knowledge to the Replacement Agency (or Government Department) to ensure similar continuity and performance of the Services post expiry of the Agreement (reference of the process).	
2.	At the end of the contract period or upon termination of contract, CSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of Government Department (reference of the process).	
3.	CSP shall support the Government Department in migration of the VMs, data, content and any other assets to the new environment created by the Government Department or any Agency (on behalf of the Government) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure. CSP shall certify the VM, Content and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered. CSP shall have the responsibility to support and assist the Government Department till the Department is able to successfully deploy and access the services from the new environment (reference of the process).	
4.	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 (reference of the process).	
5.	During the exit/transition management process, it is the responsibility of the CSP to address and rectify the problems with respect to migration of the Department application and related IT infrastructure including installation/reinstallation of the system software etc (reference of the process).	
6.	The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with Government Department (reference of the process).	
7.	During the contract period, the CSP shall ensure that all the documentation required by the Government Department for smooth transition including configuration documents are kept	

	up to date and all such documentation is handed over to the department during the exit management process (reference of the process).	

Managed Services Requirements

Applicable only when one or a combination of IaaS, PaaS, DevOps and VDaaS cloud service offerings of the private service provider (CSP) are proposed to be accredited.

The below are managed services requirements that the CSP may provide to the Government Departments.

Backup Services		
S. No.	**Nature of the Requirement**	**Compliance Statement**
1.	The CSP should 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 the policy defined by MeitY or the Government Department (reference of the process).	
2.	The CSP shall be responsible for file system and database backup and restore services. As part of the responsibilities the CSP should: (reference of the process)	
	a. Perform and store data and file backups (process of duplicating the customers "to be-backed-up" "Target Data") consisting of an initial full back up with daily incremental backups for files;	
	b. For the files, perform weekly backups;	
	c. For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files;	
	d. Encrypt all backup files and data and manage encryption keys	
	e. Monitor and manage backup activity;	
	f. The encrypted backup copy should be moved to off-site at least once daily	
	g. Restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month within a two hour timeframe for data that can be restored from a local copy;	
	h. Retain inactive versions of backed up flat files for 30 days and the last version of a deleted file for 60	

	days;	
	i. Retain database backups for thirty (30) days;	
	j. Perform administration, tuning, optimization, planning, maintenance, and operations management for backup and restore;	
	k. Provide and install additional infrastructure capacity for backup and restore, as required; and,	
	l. Perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.	
Backup Services		
1.	In addition to the Primary DC, the CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center and meet the RPO and RTO requirements. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from DC to DRC or vice -versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements (reference of the process).	
2.	The Primary DC and the DRC should be in different seismic zones (reference of the process).	
3.	The DRC can be offered from a traditional Data Center Facility and all the relevant mandatory requirements defined for the Primary Data Center as indicated below apply for the Disaster Recovery Center (reference of the process)	
	a. Deployment Model Specific Requirements as defined under Section 5.1	
	b. General Requirements as defined under Section 5.2	
	c. Service Level Agreement Management as defined under Section 5.3.2	
	d. Operational Management as defined under Section 5.3.3	
	e. Data Management as defined under Section 5.3.4	
	f. User/Admin Portal Requirements under Section 5.4	
	g. Integration Requirements under Section 5.5	
	h. LAN / WAN Requirements under Section 5.6	

	i. Data Center Facilities Requirements under Section 5.7	
	j. Security Requirements under Section 5.11	
	k. Legal Compliance Requirements under Section 5.12	
	l. Management Reporting Requirements under Section 5.13	
	m. Exit Management and Transition Requirements under Section 5.14	
4.	In case of any disaster, the security posture of the DR site shall be identical to the posture provided in the DC (reference of the process).	
5.	The disaster recovery site shall have the similar environment (physical & IT), processes, and controls (security, etc.) As that of the primary DC. During normal operations, the Primary Data Center 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 but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site (reference of the process).	
6.	In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. 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. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall 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. 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. The CSP shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from Page 44 of 81 the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss (reference of the process).	
7.	The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The 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 migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill (reference of the process).	
8.	The CSP should offer dashboard to monitor RPO and RTO of each application and database(reference of the process).	
9.	The CSP should offer switchover and switchback of individual applications instead of entire system(reference of the process).	
10.	Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities(reference of the process).	