Guidelines for User Departments on Service Level Agreement for Procuring Cloud Services

DISCLAIMER

This document has been prepared by Cloud Management Office (CMO) under the Ministry of Electronics and Information Technology (MeitY). This document is advisory in nature and aims to provide information in respect of the GI Cloud (MeghRaj) Initiative.

Certain commercial entities, technology, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by MeitY.

While every care has been taken to ensure that the contents of this document are accurate and up to date, the readers are advised to exercise discretion and verify the precise current provisions of law and other applicable instructions from the original sources. It represents practices as on the date of issue of this document, which is subject to change without notice. The readers are responsible for making their own independent assessment of the information in this document.

In no event shall MeitY or its' contractors be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of or inability to use this Document.

Table of Contents

1. Purpose

The purpose of this document is to assist Government Departments in incorporating relevant Service Level Agreement in their contractual arrangements with the Cloud Service Providers (CSPs) / Managed Service Providers (MSPs) to take care of the risks and challenges associated with the procurement and consumption of third-party Cloud services.

2. Background

It has been almost three years since the first round of empanelment of Cloud Service Offerings of Cloud Service Providers by MeitY in September 2016. During this period, a significant number of Government Departments have procured empaneled Cloud Service Offerings and consuming them. As these Government Departments, which have just embarked on their Cloud expedition, continue consuming Cloud services, they need to make sure that their information assets are adequately protected, the Cloud services being consumed by them are meeting the expected performance levels, they have sufficient controls to monitor the Cloud environments, and they are charged for the actual consumption of the Cloud services, among other assurances.

It is in this context; this document identifies service level agreements that Government Departments may include in their RFPs / contracts for procuring Cloud services. Model SLA in this document are provided for the Departments to identify critical service levels for cloud and standardize the SLA terminologies across Cloud Service providers.

In addition to the above, this document highlights the Service Level Agreement guidelines which may be considered by departments when formulating SLA section in the contracts for cloud procurement.

2.1. Empanelment of Cloud Service Offerings

MeitY has recently revised the empanelment strategy and floated additional requirements for CSPs whose Cloud services are already empaneled with MeitY. The revised strategy for empanelment of Cloud Service Offerings of CSPs is based on the three key tenets - (i) ease in offering Cloud services to government and public sector organizations, (ii) faster procurement by the government and public sector organizations, and (iii) continuous monitoring of Cloud Service Providers and their offerings. The revised empanelment strategy allows CSPs to offer Cloud services under all three categories of Cloud Service Models.

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

In the revised empanelment process, detailed audit of each CSP shall be conducted before its services are empaneled with MeitY. This audit shall be valid for a duration of three years. Thereafter, each CSP shall also undergo a surveillance audit every year for the following two requirements.

(i) Minimum security requirements specified by MeitY

(ii) Any additional requirements specified by MeitY / requirements arising out of any additional service proposed to be offered by the CSP

2.2. Guidelines for Procurement of Cloud Services

To further facilitate the end user departments in procuring/ adopting Cloud Computing services, MeitY has prepared broad guidelines highlighting key considerations that Government Departments need to be aware of when procuring Cloud services. The Cloud Procurement Guidelines may be seen on the MeghRaj webpage at https://meity.gov.in/writereaddata/files/Guidelines-Procurement_Cloud_Services.pdf.

MeitY has also prepared a document to assist government organizations in procuring Cloud services through the Government eMarketplace (GeM) platform. This document may be seen on the MeghRaj webpage at https://meity.gov.in/writereaddata/files/Guidelines_GeM_Procurement.pdf .

3. Service Level Agreement Guidelines for Procuring Cloud Service

It is best if the service level objectives offered by each cloud service provider for similar services can be easily compared. But SLA terminology, measurement methodology, metrics often differs from one cloud service provider to another, making it difficult for Government Departments/ Agencies to compare cloud service offerings and the Service Levels. In order to facilitate Government Departments, the key service level objectives are identified, described the SLAs terminologies, indicated the measurement methodology to be adopted for measuring the services, defined the metrics/target levels and penalties to be levied are indicated in case of non-performance.

However, the set of Service Level Objectives (SLOs) defined below is not exhaustive and other additional SLOs may be required specific to projects. Also certain requirements are not mentioned in the SLAs, but CSPs / MSPs are required to comply with the requirements mentioned in the empanelment RFP.

The key service level objectives that relate to the cloud service and the related aspects of the interface between the department and the cloud service provider are indicated below:

3.1. Availability

Availability may be described as the quality of being accessible and usable upon demand by an authorized entity. It is a key service level objective, since it describes whether the cloud service is actually usable / functioning. It is typically necessary to specify numeric values for availability for Government Department/ Agency to identify which services/resources are to be monitored under availability and indicate the measure of availability.

3.2. Performance

This section covers the common service level objectives that relate to the performance of the cloud service and the related aspects of the interface between the cloud service customer and the cloud service provider. Key indicative performance parameters on which SLA shall be monitored must include responsiveness of the service provider on provisioning the New VM , response time for processing a transaction and Spinning of the object & block storage etc.

3.3. Security

Security incidents could consist of any kind of Malware attacks / Denial of services / Intrusion and any kind of security breach including data theft/ loss/ corruption. Security being one of the most

Important aspects would be governed by stringent standards. All security incidents leading to disruption in availability of the Cloud Service would be penalized heavily.

3.4. Support Channel- Incident and Helpdesk

Support is an interface made available by the Service provider to handle issues and queries raised by the Government Department. As per the Cloud Service Bouquet, Cloud Service Providers will made the "Support as a service" available to be procured by the Government departments. The parameters to measure the performance of the support service does include responsive and timely resolution and reporting of the issues.

3.5. Disaster Recovery and Data Backup Management

This category is usually related to address the business continuity management and disaster recovery. Disaster recovery/ service reliability is the property of cloud service to provide the services and data availability in the acceptable form, typically over some period of time in case of any disaster. Scheduled downtime and maintenance are normally iron out while designing the service level agreements. It too covers the Service Providers capability to avoid loss of data in case of the any disaster or failures

The two primary service level agreements which needs to be addressed here are i) RPO – recovery point is the maximum allowable time between recovery points and ii) RTO – recovery time is the maximum amount of time a business process may be disrupted after the disaster.

3.6. Audit and Monitoring

Audit and Monitoring is defined as the formal and procedural approach designed to evaluate and improve the effectiveness of the process and controls.

As part of the empanelment process, MeitY has mandated CSPs to have various certifications like ISO 27001:2013 ,ISO 20000:1 , ISO 27017 , ISO 27018, TIA-942-B / UPTIME (Tier III or higher). The Service level agreements for this category will measure the sustenance of these certifications. In addition to this SLA needs to put in place with respect to the notification in case of the any disruption with respect to patch updation, budget or non-closure of the audit observation.

4. Measurement and Monitoring

The following clauses related to measurement and monitoring may be included in the RFP:

a) The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of Department or an agency designated by them, then the Department will have the right to take appropriate disciplinary actions including termination of the contract.

b) The full set of service level reports should be available to the Department on a monthly basis or based on the project requirements.

c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The Service Provider shall make available the Monitoring tools for measuring and monitoring the SLAs. The MSP may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the Department on a monthly basis. The Department or its nominated agency shall have full access to the Monitoring Tools/portal (and any other tools / solutions deployed for SLA measurement and monitoring) to extract data (raw, intermediate as well as reports) as required during the project. The Department or its nominated agency will also audit the tool and the scripts on a regular basis.

d) The measurement methodology / criteria / logic will be reviewed by the Department.

e) In case of default on any of the service level metric, the SP shall submit performance improvement plan along with the root cause analysis for the Department 's approval

5. Periodic Reviews

The SLAs might require to be modified based on the project needs. Therefore Departments need to ensure that the relevant clauses are included in the Agreement that would allow the Departments to modify the SLAs. The following clauses are provided as guidance to the departments while preparing the Service Level Agreement

a) During the contract period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology / logic / criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e. the Department and Service Provider.
b) The Department and Service Provider shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of the Department and Service Provider in accordance with the Change Control Schedule.
c) The SLAs may be reviewed on an annual basis by the Department in consultation with the Service Provider and other agencies.
d) All the SLA penalty calculation should be done for the mentioned calendar month.

6. Penalty Calculation

For the Departments to ensure that the Cloud Service Providers adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on the Service Provider. In case these service levels cannot be achieved at service levels defined in the agreement, the departments should invoke the performance related penalties. Payments to the Service Provider to be linked to the compliance with the SLA metrics laid down in the agreement. To illustrate calculation of penalties, an indicative example is provided below.

a) The payment should be linked to the compliance with the SLA metrics
b) The penalty in percentage of the Quarterly Payment is indicated against each SLA parameter
c) The Service provider will be exempted from any delays or slippages on SLA parameters arising out of following reasons:-
    I. The non-compliance to the SLA other than for reasons beyond the control of the Service Provider. Any such delays will be notified in writing to the department and will not be treated as breach of SLA from the Service provider's point of view.
    II. There is a force majeure event effecting the SLA which is beyond the control of the Service Provider.
d) The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 50% of quarterly payments, it will result in a material breach. In case of a material breach, the operator will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the Department.

7. Service Levels

S. No	Service Level Objective	Definition	Target	Penalty
Availability				
1	Availability of each cloud service (Applicable for all Cloud Service as defined in Cloud Services Bouquet)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month: (Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the cloud service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.
2	Availability of Critical Services(As defined in Annexure B) *This SLA shall not be applicable when the associated cloud service as mentioned in SLA#1 above is not available /up.	Availability means, the aggregate number of hours in any specified time period during which the critical service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month:{[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the critical service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 5% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 10% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 15% of Quarterly Payment of the Project d) <98% - 20% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.

S. No	Service Level Objective	Definition	Target	Penalty
3	Availability of regular reports (SLA , Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Penalty as indicated below (per occurrence): a) <11 working days to >= 6 working days - 2% of Quarterly Payment for the Project b) <16 working days to >= 11 working days - 4% of Quarterly Payment for the Project c) For the delay beyond 15 days , penalty of 5% of the Quarterly Payment for the Project
4	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use Uptime Calculation for the calendar month:{[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability of the Cloud Management Portal of CSP >=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the Quarterly Payment of the Project.
Performance				
5	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core) Measurement shall be done by analyzing the log files	95% within 5 minutes	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Service b) <90% to >= 85.0% - 10% of Quarterly Payment of the Service c) <85% to >= 80.0% - 15% of Quarterly Payment of the Service d) <80% - 20% of the Quarterly Payment of that Service

S. No	Service Level Objective	Definition	Target	Penalty
6	Spinning up the Object Storage	Time to spin up Object Storage Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service
7	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service
8	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports.	No more than 15 minutes lag between usage and Cloud Service (API) reporting, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project

S. No	Service Level Objective	Definition	Target	Penalty
9	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports and Invoices	No more than 24 Hrs. of lag between availability of cost details and actual usage, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project
Security				
11	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with Government Dept. within 5 working days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability reports shared with Government Dept. within 5 working days of vulnerability identification>= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project
12	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. a) High Severity - Perform vulnerability correction within 30 days of vulnerability identification. b) Medium Severity - Perform vulnerability correction within 60 days of vulnerability identification. c) Low Severity - Perform vulnerability correction within 90 days of vulnerability	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project

S. No	Service Level Objective	Definition	Target	Penalty
		identification. Measurement period is calendar month.		
13	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)	No breach	For each breach/data theft, penalty will be levied as per following criteria. 1. Severity 1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity 2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity 3 (as define in Annexure A) - Penalty of Rs 5 Lakh per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << Government Department / Agency>> reserves the right to terminate the contract.
15	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: *Malware Attack*: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. *Denial of Service Attack*: This shall include non-availability of any of the Cloud Service due to attacks that consume related resources. The Service Provider shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. *Intrusion*: Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of	a) Any Denial of service attack shall not lead to complete service non-availability. b) Zero Malware attack / Denial of Service attack / Intrusion / Data Theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the Quarterly Payment of the Project

S. No	Service Level Objective	Definition	Target	Penalty
		data. The Service Provider shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.		
Support Channels - Incident and Helpdesk				
16	Response Time under Basic Support (As defined under cloud service bouquet)	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 60 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Basic Support service
17	Percentage of timely incident report under Basic Support service(As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 1 Hr. of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Basic Support service

S. No	Service Level Objective	Definition	Target	Penalty
18	Response Time under Enterprise Support (As defined under cloud service bouquet)	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Enterprise Support service
19	Percentage of timely incident report under Enterprise Support service(As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 15 min of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Enterprise Support service
20	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 95% of the incidents should be resolved within 30 minutes of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
21	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of

S. No	Service Level Objective	Definition	Target	Penalty
			AND 95% of Severity 3 within 16 hours of problem reporting	the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
Disaster Recovery and Data Backup Management				
22	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <= 4 hours Government Department may specify more stringent RTO based on its application requirements	10% of Quarterly Payment of the Project per every additional 2 (two) hours of downtime
23	RPO (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours Government Department may specify more stringent RPO based on its application requirements	10% of Quarterly Payment of the Project per every additional 2 (two) hours of data loss
24	DR Drills	At least two DR drills in a year (once every six months) or as per the agreement	At least two DR drills in a year (once every six months) or as per the agreement	a) No of DR Drills =1 - 1% of the Yearly Payment of the Project b) No of DR Drills = 0 - 2% of the Yearly Payment of the Project

S. No	Service Level Objective	Definition	Target	Penalty
				These will be measured every six months and the liquidated damage will be levied at the end of year
25	Data Migration	Migration of data from the source to destination system	Error rate < .25%	a) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the Project b) Error Rate > 0.30% & <=0.35% - 2% of the Quarterly Payment of the Project c) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the Project For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the Project will be levied as additional liquidity damage
Audit & Monitoring				
26	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.0% - 10% of Quarterly Payment of the Project c) <85% to >= 80.0% - 15% of Quarterly Payment of the Project d) <80% - 20% of the Quarterly Payment of that Project
27	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage based threshold Measurement shall be done by analyzing the log files	99% within 10 mins of crossing the Threshold	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 0.25% of Quarterly Payment of the Project b) <95% to >= 90.0% - 0.5% of Quarterly Payment of the Project c) <90% to >= 85.0% - 0.75% of Quarterly Payment of

S. No	Service Level Objective	Definition	Target	Penalty
				the Project d) <85% - 1% of the Quarterly Payment of that Project
28	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project duration. Service Provider should ensure the sustenance / renewal of the certificates	All certificates should be valid during the Project duration	Delay in sustenance of certifications a) > 1 day & <= 5 days - 1% of the Quarterly Payment of the Project b) > 5 day & <= 15 days - 2% of the Quarterly Payment of the Project c) > 15 day & <= 30 days - 5% of the Quarterly Payment of the Project d) > 30 days, 10% of the Quarterly Payment of the Project
29	Non-closure of audit observations	No observation to be repeated in the next audit	All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 5% of the Quarterly Payment of the Project b) > 10 % & <= 20% - 10% of the Quarterly Payment of the Project c) > 20 % & <= 30% - 20% of the Quarterly Payment of the Project d) >30% - 30% of the Quarterly Payment of the Project

Annexure A – Severity Levels

Below severity definition provide indicative scenarios for defining incidents severity. However Government Department/Agency will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

Severity Level	Description	Examples
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	• Non-availability of VM. • No access to Storage, software or application
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	• Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

Annexure B – Definitions

I. **Critical Services:** Critical service may be defined as Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Security Components, etc.

II. **Business Hours**: Business hours may be referred as prime business period, which shall be from 08:00 A.M IST till 10:00 PM IST on all days.