"RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) Site for MITL on Cloud"."

Tender No- MITL/ICT/2026-27/001 **Date: 04th Aug 2024**

Corrigendum-1

The terms and conditions of RFP cum RFQ documents of tender are modified as under:

Sr. No.	Reference Clause	RFP Clause	Revised clause
1	**General**	Definition clause for the RFP	Please refer to the attached Bidder in Annex-V to Corrigendum-1 and shall supersede the corresponding provisions of the original RFP.
2	**Clause - 2.7, page no-20 : Performance Bank Guarantee**	Performance Bank Guarantee (PBG) of value of 10% of the Contract Value need to be provided by the successful bidder as per the format given in RFP. PBG should be drawn on Nationalised / Scheduled Bank for 5 years with additional claim period of 1 year from the date of expiry providing for encashment at Mumbai Branch.	Performance Bank Guarantee (PBG) of value of 10% of Contract Value need to be provided by the successful bidder as per the format given in RFP. PBG should be drawn on Nationalised / Scheduled Bank for 26 Months with additional claim period of 1 year from the date of expiry providing for encashment at Mumbai Branch.
3	**GCC000, page-91**	The Performance Security shall be denominated in the currency of the contract for an amount equal to 3% of the contract value (Grand Total/Evaluated Bid Price (C) as per Form 1.3 of Financial Proposal) including taxes in INR.	The Performance Security shall be denominated in the currency of the contract for an amount equal to 10 % of the contract value.
4	**Clause 9.2.2 , page no-43**	DRC / Secondary DC	The revised Penalty Terms and Service Level Agreement (SLA) Matrix are attached as Annexure-I to Corrigendum-1 and shall supersede the corresponding provisions of the original RFP.
5	**Clause 14, page no SLA**	Penalty Terms for Quality of Services	The revised Penalty Terms and Service Level Agreement (SLA) Matrix are attached as Annexure-I to Corrigendum-1 and shall supersede the corresponding provisions of the original RFP.
6	**Clause 17.12, page no-131**	Monthly Cost for Disaster Recovery Centre (DRC) / Secondary Data Centre (DC) Costs (Not to be Evaluated)	The Revised Monthly Charges for the Disaster Recovery Centre (DRC) / Secondary Data Centre (DC) are attached as Annexure-II to Corrigendum-1. These charges are for reference only and shall not be considered for bid evaluation. MITL reserves the right to avail the DRC/Secondary DC services in the future at the rates quoted by the successful bidder, if required.

7	**Clause No-16, Cloud Infrastructure Requirement, page no- 127**	**Network Connectivity & Security** 1. Web Application Firewall 2. SIEM (Security Incident and Event Management) to monitor security incidents.	The function requirement is attached in Annex-III to Corrigendum-1 and shall supersede the corresponding provisions of the original RFP.
8	**3.1.3, Infrastructure Analysis and Build , page no-22**	CSP shall provide Backup solution with different features, like snapshots of VMs, RDBMS backup, incremental and full back up of all data, restoration of data in test environment or as and when required.	The function requirement is attached in Annex-IV to Corrigendum-1 and shall supersede the corresponding provisions of the original RFP.

Annex-I

Penalty Terms for Quality of Services

For the MITL to ensure that the Cloud Service Provider adhere to the Service Level Agreement. In case these service levels cannot be achieved at service levels defined in the agreement, the MITL will invoke the performance related penalties.

All the SLA related terms are explained in the SLA agreement.

The penalty in the percentage of the Quarterly payment has been as indicated against each SLA parameter in the table.

Service Level Objective	Measurement	Target Service Level	Penalty Clause
Availability/Uptime of cloud services and Resources for CSP's Infrastructure	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components, orchestration layer, virtualization layer) provisioned in the cloud. Measured with the help of SLA reports provided by CSP	<99.95% & >=99.5%	1% of Quarterly Payment
		< 99.5% & >=99%	2% of Quarterly Payment
		Subsequently, every 0.5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting - Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. Quarter). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	<95% and >=90% within 1 hour	1% of Quarterly Payment
		<90% and >=85% within 1 hour	2% of Quarterly Payment
		Subsequently, every 5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting – Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (quarter) over the total number of defined incidents to the cloud service within a predefined period (quarter). Measured from Incident Reports	<95% and >=90% within 1 hour	1% of Quarterly Payment
		<90% and >=85% within 1 hour	5% of Quarterly Payment
		Subsequently, every 5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.).	<99.95% and >=99	1% of Quarterly Payment
		<99% and >=98%	2% of Quarterly Payment
		Subsequently, every 1% drop in SLA criteria	Additional 2% of Quarterly Payment till event of default and termination

Service Level Objective	Measurement	Target Service Level	Penalty Clause
	1. High Severity Vulnerabilities – 30 days - Maintain 99.95% service level 2. Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level		
Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.).	<99.95% and >=99	1% of Quarterly Payment
		<99% and >=98%	2% of Quarterly Payment
		Subsequently, every 1% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Security and Privacy breach including Data Theft / Loss/ Corruption/Mining	Any incident where in system compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents)	No breach	For each breach / data theft / data corruption / data mining issue / privacy breach, penalty will be levied as per the following criteria. Any confirmed security incident, established by root cause analysis to be attributable to an act, omission or negligence of the CSP – INR 2 Lakhs. This penalty is applicable per incident. The aggregate of all penalties levied under this head in any quarter shall not exceed 10% (ten percent) of the Quarterly Payment for that quarter, and shall form part of, and be counted towards, the overall SLA penalty cap per quarter. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, Client reserves the right to terminate the contract.
Meeting Recovery Time Objective (RTO) (If Secondary DC / DRC as a Service is taken by the Client)	Measured during the regular planned or unplanned (outage) changeover from DC to secondary DC / DRC or vice versa.	As per project requirement given in Scope of Work. If it exceeds as per below following penalties to be levied	
		RTO – 4 hours	1% of Quarterly Payment shall be deducted
		For every increase of 30 mins in RTO	Additional 2% of Quarterly Payment till event of default and termination
Meeting Recovery Point	Measured during the regular planned or unplanned (outage)	As per project requirement given in Scope of Work. If it	

Service Level Objective	Measurement	Target Service Level	Penalty Clause
Objective (RPO)_ (If Secondary DC / DRC as a Service is taken by the Client)	changeover from DC to secondary DC / DRC or vice versa	exceeds as per below, following penalties to be levied	
		RPO – 2 hours	1% of Quarterly Payment shall be deducted
		For every increase of 30 mins in RPO	Additional 2% of Quarterly Payment till event of default and termination
Availability of the network links at DC and DR/Secondary DC (If Secondary DC / DRC as a Service is taken by the Client)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%	No Penalty
		<99.5 and => 99%	1% of quarterly payment
		<99 and => 98.5%	2% of quarterly payment
		<98.5%	3% of quarterly payment

Service Level Agreement

Meity has announced MeghRaj Policy to provide strategic direction for adoption of cloud services by the Government. The aim of the cloud policy is to realize a comprehensive vision of a government cloud (GI Cloud) environment available for use by central and state government line departments, districts and municipalities to accelerate their ICT-enabled service improvements. MeghRaj policy of Meity states that "Government departments at the Centre and States to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects may be evaluated to assess whether they should migrate to the GI Cloud."

1.1 Purpose

- The purpose of Service Levels is to define the levels of service provided by the Cloud Service Provider ("CSP") to MITL ("Client") for the duration of the contract. The benefits of this are:
    - Help the Client control the levels and performance of CSP's services.
    - Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.
- The Service Levels are between the Client and CSP.

1.2 Service Level Agreements & Targets

- This section is agreed to by Client and CSP as the key performance indicator for the project.
- The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of Contact.

1.3 General Principles of Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the CSP. SLA defines the terms of CSP's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The CSP shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

"Total Time" – Total number of hours in the quarter being considered for evaluation of SLA performance.

"Downtime" – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the CSP.

"Scheduled Maintenance Time"– Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The CSP shall seek at least

15 days' prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.

"Uptime" – Time period for which the specified services are available in the period being considered for evaluation of SLA.

Uptime (%) = (1- {[Total Downtime] / [Total Time- Scheduled Maintenance Time]}) * 100. Penalties shall be applied for each criterion individually and then added together for the total penalty for a particular quarter

"Incident" – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.

"Response Time" – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.

"Resolution Time" – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

"Target" – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/(Total time in quarter)]*100.

Latency: Latency may address the storage and the time when the data is placed on mirrored storage.

Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.

Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.

Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.

Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)

Penalty shall be applied for each criterion individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

1.4 Service Levels Monitoring

- The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.
- As part of the Project requirements, CSP shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the CSP for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.
- The CSP will endeavour to exceed these levels of service wherever possible.

- CSP undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.
- CSP will provide a supplemental report on any further information received, as soon as the information becomes available.
- CSP will take instruction only from authorized personnel of the Client.
- In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.
- For issues i.e. breach of SLAs beyond control of the CSP, the CSP shall submit a justification for the consideration of the Client. In case it is established that the CSP was responsible for such breach, respective penalty shall be applied to the CSP.

1.5 Measurements & Targets - Operations Phase SLAs

- These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.
- The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.
- CSP's published SLAs and penalties shall be also being applicable during the course of the Contract.
- The following SLAs apply for CSP. While the CSP will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the CSP will be responsible for the SLAs related to managing and monitoring the cloud services.

Sr.no	Parameter	Metric	Penalty
1	Database Server Uptime Application Server Uptime Web Server Uptime SAN Storage Uptime Internet Link Any other IT component in the Infrastructure Architecture	>=99.95%	Per 0.5% breach of target penalty shall be Rs. 10,000. Maximum penalty of 5 % of quarterly payment amount. Penalty will be deducted from the quarterly payments.

1.6 Severity Level

Below severity definition provide scenarios for incidents severity.

Severity Level	Description
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
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.

Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.

Sr. No	Parameter	Description	Threshold
1	Response Time	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 15minutes
2	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 60 minutes of problem reporting
3	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 & 95% of Severity 3 within 16 hours of problem reporting

Annex II

Optional Rate Card for Discovery of Unit Rates (Additional Line Items)

The following rate card is for the purpose of discovering firm unit rates for additional/future line items that the Department may require during the contract period. The tentative quantity of one (1) against each item is indicative only and does not constitute any committed procurement by the Department.

The rates quoted in this rate card shall **not** form part of the evaluated commercial bid for QCBS evaluation; the commercial score shall be computed solely on the GRAND TOTAL of the Bill of Material above. The Department reserves the right to procure any quantity of these items, at the quoted unit rates, on an as-required basis during the contract period and any extension thereof.

All rate-card unit rates shall remain firm and shall be treated as ceiling rates for the duration of the initial contract period. For any item that also appears in the Bill of Material, the unit rate quoted in this rate card shall not exceed the equivalent unit rate derived from the Bill of Material. Any item left blank or quoted as zero/nil shall be treated as included at no extra cost. In the event the contract is extended under the Extension of Contract clause, the rate-card unit rates applicable during the extension period shall be mutually agreed in writing between the Department and the CSP prior to commencement of the extension, in the same manner as the other prices under the contract.

Sr. No	Item Title	Item Description	Tentative Quantity *	Unit of Measure	Unit Price (Inclusive of all taxes)
1	vCPU (1:1)	Per Virtual Core	1	No	
2	vCPU (1:2)	Per Virtual Core	1	No	
3	vRAM	Per GB Virtual RAM	1	No	
4	Block Storage	All SSD (1000	1	TB	
5	Performance Storage	All SSD (3000	1	TB	
6	Performance Storage	All SSD (5000	1	TB	
7	Archive Storage	SAS/NL SAS	1	TB	
8	Backup Storage	SAS/NL SAS	1	TB	
9	Windows OS (2 vCores/License)	Latest	1	No	
10	Public IP	IPv4/IPv6	1	No	
11	Host Intrusion Prevention system	Per VM	1	No	
12	Cloud Monitoring Service	Per Device	1	No	
13	MS SQL Std (2 vCores/License)	Latest	1	No	
14	MS SQL Ent (2 vCores/License)	Latest	1	No	
15	Virtual Load Balancer	1 Gbps	1	No	
16	Cross Connect	Per termination	1	No	
17	Unmetered Internet Bandwidth	Unmetered per Mbps	1	Mbps	
18	DNS Entry	Per Instance	1	No	
19	Virtual UTM along with 25 SSL VPN for Desktop or Laptop	1Gbps throughput	1	No	
20	Virtual Web Application Firewall	1Gbps throughput	1	No	
21	Vulnerability Assessment and Management Service/tool	Per URL/Domain	1	No	
22	DDoS as a service	Gbps Mitigation	1	No	
23	Postgres Enterprise (Unicore)	Latest	1	No	
24	Postgres Community	Latest	1	No	
25	MY SQL Std	Latest	1	No	
26	CERT-IN Empaneled VAPT	Per Device	1	No	

27	Domain Wildcard SSL Certificate	Per Domain	1	No	
28	Domain SSL Certificate	Per Domain	1	No	
29	MY SQL Community	Latest	1	No	
30	DRM Tool	Per VM	1	No	
31	Replication link between DC and DR	Per Mbps	1	MBPS	
32	Backup Agent	Per VM	1	No	
33	EDR	Per Device	1	No	
34	SSL VPN	Per User	1	No	
35	Enterprise Email as a Service	Per Mailbox	1	No	
36	Storage Managed Services	Per TB	1	No	
37	Backup Managed Services	Per VM	1	No	
38	Archival Managed Services	Per VM	1	No	
39	vFirewall Managed Services	Per vFW	1	No	
40	vWAF Managed Services	Per vWAF	1	No	
41	vLB Managed Services	Per vLB	1	No	
42	Database Managed Services	Per 100 GB	1	No	
43	OS Managed Services	Per OS	1	No	
44	Application Performance Monitoring tool – perpetual Licnses	Per Web/App server	1	No	
45	Database Performance Monitoring Tool – perpetual License	Per DB server	1	No	
46	Database activity Monitoring	Per DB instance	1	No	
47	CDN as a Service	Per TB	1	No	
48	email gateway	Per 1 Lac Email	1	No	
49	SMS gateway	Per 1 Lac SMS	1	No	
50	RHEL Small and Large Instance	Latest	1	No	
51	CENT OS	Latest	1	No	
52	Patch Management	Latest	1	No	
53	SIEM as a Service	Devices in infrastructure	1	No	
Total				**Rs.**	

All unit rates are exclusive of all applicable taxes, duties and levies, and are firm/ceiling rates for the initial contract period. Rates applicable during any extension period shall be as mutually agreed under the Extension of Contract clause.

Annex III

CSP technical and functional compliance for Key components and operations

Web Application Firewall

#	Description	Compliance (Y/N)
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection	
2	Service provider WAF should be able to support multiple website security.	
3	Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.	
4	Service provider WAF should be able to block invalidated requests.	
5	Service provider WAF should be able to block attacks before it is posted to website.	
6	Service provider WAF should have manual control over IP/Subnet. i.e., Allow or Deny IP/Subnet from accessing website.	
7	The attackers should receive custom response once they are blocked.	
8	Service provider must offer provision to customize response of vulnerable requests.	
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10	Service provider WAF should be able to Whitelist or Backlist IP/Subnet.	
11	Service provider WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceed the threshold limit.	
12	The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.	
13	WAF should be able to set a limit to maximum file size, combined file size in bytes	
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions & headers	
15	Service provider WAF should be able to limit maximum number of arguments, argument name, value, value total length etc.	
16	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.	
17	Should be able to limit maximum size of request body entity in bytes	
18	The WAF should be able to close all the sessions of an IP if it is ban.	
19	Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.	
20	The WAF access and security Dashboard should show a graphical representation of	

#	Description	Compliance (Y/N)
	A) For access report analysis purpose the Dashboard should contain following information:	
	i) Number of hits by status code	
	ii) HTTP status code wise hits	
	iii) HTTP methods wise hits	
	iv) Client browser wise hits	
	v) Client Operating system wise hits	
	vi) Traffic(No. of hits) per URL	
	vii) Average bytes received per request	
	viii) Average bytes sent per request	
	ix) Average time elapsed per request	
	B) For security report analysis purpose the Dashboard should contain following information:	
	i) Average score by status code	
	ii) Distribution of blocked requests	
	iii) Number of blocked requests	
	iv) OWASP Top 10 requests	
	v) Reputation tags	
	vi) IP list reputation	
	C) For network incoming and outgoing traffic captured by WAF packet filter dashboard should contain following information:	
	i) Number of packet hits	
	ii) Source IP, Destination IP wise hits	
	iii) Firewall actions(allow, deny) wise hits	
	iv) Requests per destination port wise hits	
	D) Geo map of number of hits by country	
21	WAF should support different policies for different web applications.	
22	Vendor to ensure 24x7x365 availability of WAF service.	
23	WAF should support different policies for different application section (different security zones within the app).	
24	WAF should support IP Reputation DB (DB including blacklisted IP Address, IP Address, Anonymous Proxy, Botnets, Windows Exploit etc.) along with Client Source IP address based Security Policy and dynamic source IP blocking.	
25	WAF should enforce file upload control based on file type, size etc.	
26	WAF should detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses or anonymous proxy addresses.	
27	WAF should support detection only, blocking and transparent mode.	
28	WAF solution should be capable of handling IPV4 and IPV6 traffic.	

#	Description	Compliance (Y/N)
29	WAF solution should ensure compliance and advanced protection against industry standards such as OWASP Top 10 vulnerabilities etc.	
30	Vendor must monitor, manage & maintain the WAF solution on a 24x7 basis.	
31	WAF should provide a real-time dashboard with data such as top attacks view, traffic monitoring view, etc.	
32	WAF should provide role based access control for the dashboard (role based multiple login accounts both primary and secondary to be provided).	
33	WAF should provide detailed reports for all web application attacks.	
34	WAF should be able to decrypt the SSL traffic to analyse the HTTP data and should be able to re-encrypt the SSL traffic.	
35	WAF should support SSL offloading.	
36	WAF should support body inspection, content injection, backend compression, validation of UTF8 Encoding, XML Inspection.	
37	WAF should block invalid BODY.	
38	WAF should log all transactions for auditing purpose.	
39	WAF should block desktop users User-Agent, crawlers User-Agent, suspicious User-Agent.	
40	WAF should have customizable scoring policy for each request and can block request if global score exceeds.	
41	WAF should have DOS and BF protection for all or specific URLs.	
42	WAF should have learning mode to create whitelist/blacklist rules and also block attack in learning mode.	
43	WAF should verify SSL certificate, certificate name, expiration and cipher suites. Also control over accepted TLS/SSL protocol, cipher order, CRL verification, HTTP public key pinning, OCSP stapling.	
44	WAF should allow to inject Request and Response headers for applications.	
45	WAF should support Content and URL rewriting policies.	
46	WAF should send proxy HTTP headers to backend, r rewrite cookie path, backend’ s cookies encryption and override backend server HTTP errors.	
47	WAF should support force HTTP to HTTPS redirection.	
48	WAF should support URL specific rulesets and should allow/deny specific countries(GeoIP) for applications.	
49	WAF should have OS level firewall to PASS/BLOCK traffic inbound/outbound traffic	
50	WAF should allow to create custom rules for application.	
51	WAF should support Active-Active/Active-Passive failover.	

SIEM Service

Sr. No.	SIEM Description	Compliance (Y/N)
1	The solution should be able to handle a minimum of Avg 5.06 Eps / Device	
2	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.	
3	The solution should be capable of real time analysis and reporting.	
4	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
5	The solution should be able to assign risk scores to your most valuable asset. The risk value could be assigned to a service, application, specific servers, a user or a group. The solution should be able to assign and consider the asset criticality score before assigning the risk score.	
6	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.	
7	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.	
8	The SIEM receiver/log collection appliance must be an appliance based solution and not a software based solution to store the data locally, if communication with centralized correlator is unavailable.	
9	The solution should be able to collect logs via the following ways as inbuilt into the solution: Syslog, OPSec, agent-less WMI, RDEP, SDEE, FTP, SCP, External Agents such as Adiscon.	
10	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
11	The solution should provide a data store which is compressed via flexible aggregation logic.	
12	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.	
13	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.	
14	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.	
15	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.	
16	The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.	
17	A well-defined architecture along with pre and post installation document need to be shared by the bidder.	
18	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.	
19	The solution should support collection of events/logs and network flows from distributed environment(s).	

Sr. No.	SIEM Description	Compliance (Y/N)
20	The solution should correlate security/network events to enable the SOC to quickly prioritize it's response to help ensure effective incident handling.	
21	The solution should integrate asset information in SIEM such as categorization, criticality and business profiling and use the same attributes for correlation and incident management.	
22	The solution should provide remediation guidance for identified security incident:	
23	a) Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis/remediation.	
24	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.	
25	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
26	The solution should perform regular (at least twice a year) health check and fine tuning of SIEM solution and should submit a report.	
27	The solution should share the list of out of the box supported devices/log types.	
28	The solution should support hierarchical structures for distributed environments. The solution should have capability for correlation of events generated from multiple SIEM(s) at different location in single management console.	
29	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
30	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP or similar ports should not be used.	
31	Event dropping/caching by SIEM solution is not acceptable and same should be reported and corrected immediately.	
32	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.	
33	The solution should be able to capture all the fields of the information in the raw logs.	
34	The solution should support storage of raw logs for forensic analysis.	
35	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	
36	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
37	The solution should support configurable data retention policy based on organization requirement.	
38	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.	
39	The solution should compress the logs by at least 70% or more at the time of archiving.	
40	The solution should have capability for log purging and retrieval of logs from offline storage.	
41	Solution should be capable of replicating logs in Synchronous as well as Asynchronous mode for replication from Primary site to DR site.	

Sr. No.	SIEM Description	Compliance (Y/N)
42	The solution should provide proactive alerting on log collection failures so that any potential loss of events and audit data can be minimized or mitigated.	
43	The solution should provide a mechanism (in both graphic and table format) to show which devices and applications are being monitored and determine if a continuous set of collected logs exist for those devices and applications.	
44	The solution should support automated scheduled archiving functionality into file system.	
45	The solution should support normalization of real time events.	
46	The solution should provide a facility for logging events with category information to enable device independent analysis.	
47	The platform should be supplied on Hardened OS embedded in Hardware / Virtual Appliance. The storage configuration should offer a RAID configuration to allow for protection from disk failure.	
48	The platform should have High Availability Configuration of necessary SIEM components to ensure there is no single point of failure. Please describe the architecture proposed to meet this requirement.	
49	By default at the time of storage, solution should not filter any events. However, solution should have the capability of filtering events during the course of correlation and report generation.	
50	The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.	
51	The solution should be able to continue to collect logs during backup, de-fragmentation and other management scenarios.	
52	The solution should support collection of logs from all the devices quoted in RFP.	
53	The collection devices should support collection of logs via the following but not limited methods:	
54	1. Syslog over UDP / TCP	
55	2. SNMP	
56	3. ODBC (to pull events from a remote database)	
57	4. FTP (to pull a flat file of events from a remote device that can't directly write to the network)	
58	5. Windows Event Logging Protocol	
59	7. NetBIOS	
60	The solution should allow a wizard / GUI based interface for rules (including correlation rules) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.	
61	The solution should support all standard IT infrastructure including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, LDAP, Internet Gateway, Antivirus, and Enterprise Messaging System, Data loss prevention (DLP) etc.	
62	The solution should have provision for integration of the following:	
63	d) Inclusion of "Application context".	
64	Solution should have license for minimum 10 users for SIEM administration.	

Sr. No.	SIEM Description	Compliance (Y/N)
65	The solution should have the ability to define various roles for SIEM administration, including but not limited to: Operator, Analyst, SOC Manager etc. for all SIEM components.	
66	The solution should support SIEM management process using a web based solution.	
67	The solution should support the following co- relation:	
68	Statistical Threat Analysis - To detect anomalies.	
69	Susceptibility Correlation - Raises visibility of threats against susceptible hosts.	
70	Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities	
71	Rules based Correlation - The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios.	
72	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts.	
73	The solution should provide ready to use rules for alerting on threats e.g., failed login attempts, account changes and expirations, port scans, suspicious file names, default usernames and passwords, High bandwidth usage by IP, privilege escalations, configuration changes, traffic to non-standard ports, URL blocked, accounts deleted and disabled, intrusions detected etc.	
74	The solution should support the following types of correlation conditions on log data:	
75	a) One event followed by another event	
76	b) Grouping, aggregating, sorting, filtering, and merging of events.	
77	c) Average, count, minimum, maximum threshold etc.	
78	Solution should provide threat scoring based on:	
79	a) Host, network, priority for both source	
80	& destination	
81	b) Real-time threat, event frequency, attack level etc.	
82	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.	
83	The solution should have the capability to send notification messages and alerts through email, SMS, etc.	
84	The solution should support RADIUS and LDAP / Active Directory for Authentication.	
85	The solution should provide highest level of enterprise support directly from OEM.	
86	The solution should provide a single point of contact directly from OEM for all support reported OEM.	
87	The solution should ensure continuous training and best practice updates for onsite team from its backend resources.	
88	Solution should support log integration for IPv4 as well as for IPv6.	
89	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert/retrieval time, resource utilization details etc.	
90	Solution should support at least 100 default correlation rules for detection of network threats and attacks. The performance of the solution should not be affected with all rules enabled.	

Sr. No.	SIEM Description	Compliance (Y/N)
91	The central management console/ Enterprise Security managers/receivers should be in high availability.	
92	24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	
93	Recording and analysing data sources (e.g. system status, failed authentication attempts, etc.)	
94	24/7 contactable security incident handling and troubleshooting team with the authority to act	
95	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	
96	Provision of relevant log data in a suitable form	
97	Logging and monitoring of administrator activities	

Annex IV

Backup & Restore Service

- CSP shall provide backup solution (Disk / Tape based backups), covering but not limited to daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.
- CSP shall cover (not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.
- CSP shall Configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy/procedure/plan finalized by department.
- CSP shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
- The disk-based backup solution must have the feature to integrate with any Tape Library.
- CSP should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
- The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.
- Department should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.
- CSP shall restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month for data that can be restored from a local copy.
- CSP shall Provide and install additional infrastructure capacity for backup and restore.
- There has to be provision if required to shift the backup at department required location on tape/USB.
- CSP shall perform restoration testing biannually with the permission of department.
- CSP must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
- CSP shall ensure prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
- CSP shall perform Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- The backup service must provide following capabilities.
    - Compression: Support compression of data at source before backup
    - Encryption: Support at least 128-bit encryption at source
    - Alert: Support email notification on backup job's success / failure
- File exclusion: Ability to exclude specific files, folders, or file extensions from backup
- Deduplication: Provide deduplication capabilities
- Backups should be stored in such a way that disaster should not result in loss of backups.
- Indicative Backup plan

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

Annex V

Definition :- Managed Service Provider and Cloud Service Provider

For the purposes of this RFP and the Contract arising from it, the Managed Service Provider ("MSP") and the Cloud Service Provider ("CSP") shall be one and the same legal entity. The Bidder shall itself be the Cloud Service Provider empanelled with the Ministry of Electronics and Information Technology (MeitY) under the Government Community Cloud (GCC) category, and shall itself deliver the managed services set out in this RFP from its own MeitY-empanelled data centres.

Accordingly, wherever this RFP uses the expressions "MSP", "CSP", "CSP/MSP", "Service Provider" or "Successful Bidder", each such expression shall be read as referring to the same single entity, and every obligation, eligibility requirement, service level, penalty and liability stated against any one of those expressions shall bind that entity in full.

Bids submitted as a consortium, joint venture, or on a prime-and-subcontractor basis in which the managed services and the underlying cloud infrastructure are provided by different legal entities, shall not be accepted. This clause does not apply to the Master System Integrator (MSI) or the e-LMS System Integrator (SI) referred to in Section 10.3, who are separate parties appointed by the Client and are not part of the MSP/CSP scope.