RFP for selection of Service Provider for providing Cloud Services

Reference number: PSeGS/Cloud/2018/1

Punjab State e-Governance Society (PSeGS),
O/o Department of Governance Reforms (DGR),
Government of Punjab
Plot D-241, Industrial Area, Phase – 8B, Sector – 74,
Near Quark City, Mohali - 160071

Table of Contents

1. Notice Inviting Tender ***4***

2. Document Control Sheet ***5***

3. Definitions ***6***

4. Introduction ***9***

4.1. Background **9**

4.2. Invitation For Bid **9**

5. Instructions to Bidders ***12***

5.1. General **12**

5.2. Validity of Bids **12**

5.3. Tender Document Fees **12**

5.4. Amendment to the Tender Document **13**

5.5. Clarifications on submitted bids **13**

5.6. Earnest Money Deposit (EMD) **13**

5.7. Preparation of Bid **14**

5.8. Disqualifications **16**

5.9. Deviations **16**

5.10. Clarification on Tender Document **17**

5.11. Bid Opening and Evaluation **17**

5.12. Bid Evaluation **18**

5.13. Pre-qualfication / Eligibility Evaluation **18**

5.14. Technical Evaluation **21**

5.15. Commercial Bids Evaluation **22**

5.16. Notification of Award of Contract **23**

5.17. Performance Security **23**

5.18. Signing of Contract **25**

5.19. Work orders **25**

5.20. Fraud and Corrupt /Malpractices **26**

6. Scope of Work ***28***

6.2. Scale-up and scale-down of resources.....31

6.3. Role of CSP, Supplier and Client.....32

6.4. Cloud Services.....34

6.5. Disaster Recovery Services.....34

6.6. Migration Services.....34

6.7. Cloud Managed Services.....36

6.8. Exit Management Services.....37

7. General Contract Conditions.....39

7.1. Standards of Performance.....39

7.2. Contract Period.....39

7.3. Prices.....39

7.4. Additional Services.....40

7.5. Payment Terms.....40

7.6. Applicable Law.....41

7.7. Governing Language.....42

7.8. Taxes and Duties.....42

7.9. Data Ownership and Confidentiality.....42

7.10. Termination of Contract or Work Orders.....42

7.11. Exit Management.....44

7.12. Force Majeure.....45

7.13. Resolution of Disputes.....46

7.14. Legal Jurisdiction.....47

8. Bid Formats.....48

8.1. Form-1: Covering Letter for participating in the bidding process.....49

8.2. Form 2: Eligibility Criteria Form.....52

8.3. Form 3: CSP Compliance Form.....53

8.4. Form 4: Commercial Bid Form.....54

8.5. Annexure A: Performance Bank Guarantee.....55

8.6. Annexure B: Capabilities requirement for Cloud Services.....57

8.7. Annexure C: SLA and Penalties.....63

1. Notice Inviting Tender

Government of Punjab

RFP Reference Number: PSeGS/Cloud/2018/01

Punjab State e-Governance Society (PSeGS) invites online bids for the selection of Service Provider for providing Cloud Services for various e-Governance projects of Punjab.

Closing date and time is 18.10.2018 at 03.00 PM.

For details log on to www.dgrpunjab.gov.in and www.eproc.punjab.gov.in.

2. Document Control Sheet

Sl. No.	Particular	Details
1.	Document Reference Number	PSeGS/Cloud/2018/1
2.	Date & time for the start of sale of e-tender	25-09-2018 09:00 Hrs
3.	Last Date and Time for submission of queries	05-10-2018 11:00 Hrs
4.	Date and Time for Pre-Bid Meeting	05-10-2018 11:00 Hrs
5.	Last date and time for submission of bids	18-10-2018 15:00 Hrs
6.	Date and time of opening of Pre-Qualification bids	22-10-2018 11:00 Hrs
7.	Date of opening of commercial bids	To be intimated later
8.	Address for Communication	Punjab State e-Governance Society, O/o Department of Governance Reforms, Plot D-241, Industrial Area, Phase – 8B, Sector – 74, Near Quark City, Mohali - 160071
9.	Location of tender document	Tender document can be downloaded from the website https://eproc.punjab.gov.in/
10.	Cost of tender document & Mode of Payment	Rs. 5,000/- (Rs. Five Thousand Only) through online mode.
11.	Earnest Money Deposit (EMD) through online mode	Rs. 2,00,000/- (Rs. Two Lakh Only)
12.	Contact details	Mr. Dhiraj Saini Mobile : +91 7888805080 Email: dhiraj.saini@punjab.gov.in
13.	Website for RFP Reference	https://eproc.punjab.gov.in/ and dgrpunjab.gov.in

Note:

2.1.1. In case a holiday is declared on any day, the event will be shifted to the next working day, same time.

2.1.2. All corrigendum /addendums /clarifications regarding this RFP shall be posted on the above mentioned websites only. No other communication or advertisement will be given.

3. Definitions

Unless the context otherwise requires, the following terms whenever used in this tender and contract have the following meanings:

3.1.1. Cloud, as per NIST definition, is offered as on-demand self-service where the Client can unilaterally provision computing capabilities without requiring human interaction from the cloud service provider (CSP). CSP offers a set of services through their online administrative console through which the customers can unilaterally provision the compute instances (virtual machines), mount storage, configure network topology (e.g., configuration of firewalls, sub-nets, routing tables, network ACLs, private IP range, VPN gateways), and enable the right security architecture (e.g., encryption, web application firewall) as required for their environment.

3.1.2. "PSeGS" means Punjab State e-Governance Society.

3.1.3. "Bidder" means firm / company / business entity which submits bid in response to this RFP for Supply of cloud services.

3.1.4. "Committee" means the committee constituted by the PSeGS for evaluation of bids.

3.1.5. "Client" means PSeGS and / or the user department / organization of Government of Punjab.

3.1.6. "Qualified and Responsive bidders" refers to the bidders who are technically and financially qualified They must have quoted a price for any of the items in the financial bid. Contract would be signed with each such Qualified and Responsive bidder.

3.1.7. "Contract" means the contract entered between the PSeGS and the "Qualified and Responsive bidders" for supply of cloud services with the entire documentation specified in the RFP.

3.1.8. "Supplier" means the "Qualified and Responsive bidder", who is selected through L1 process as laid out in clause 4.19 of this RFP, for Supply of cloud services to the Client under the contract. Separate

"Supplier" may get selected for each requirement of the Client based on the L1 process.

3.1.9. "Work Order" refers to the work order issued by the Client to the Supplier selected by the Client for their requirement.

3.1.10. "Bids" means proposal or bid submitted by bidders in response to this tender issued by PSeGS for selection of "Supplier".

3.1.11. "EMD" means "Earnest Money Deposit".

3.1.12. "PBG" means "Performance Bank Guarantee".

3.1.13. "CSP" means Cloud Service Providers (CSP) having a valid MeitY, GoI empanelment to provide cloud services. A CSP can bid directly or authorize their partners for the bidding.

3.1.14. "Similar Work" means providing services related to Data Center or cloud.

3.1.15. Cloud "Service Level Objective" (SLO) means the target for a given attribute of a cloud service that can be expressed quantitatively or qualitatively.

3.1.16. Cloud "SLAs" means documented agreement between the Supplier and PSeGS, which identifies services and cloud service level objectives (SLOs).

3.1.17. "Response time" is the time interval between Client initiated event (e.g., logging of the request) and the Supplier initiated event in response to that stimulus.

3.1.18. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of the Client, during non-business hours. The Scheduled Maintenance time within 10 hours a month shall not be considered for SLA Calculation.

3.1.19. "Scheduled operation time" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.

3.1.20. "Availability" means the time for which the cloud services and facilities are available for conducting operations on the Client system. Availability is defined as:

{(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%

3.1.21. "Incident" refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the Client to the Supplier.

3.1.22. Recovery Point Objective is the maximum allowable time between recovery points.

3.1.23. Recovery Time Objective is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences.

4. Introduction

4.1. Background

4.1.1. Department of Governance Reforms (DGR), Punjab with the help of its implementing agency Punjab State e-Governance Society (PSeGS) administers the implementation of e-Governance projects for the overall benefit of the citizens and public by setting up the necessary administrative, financial, legal and technical frameworks, implementation mechanisms and resources for various government departments in the State of Punjab.

4.1.2. Numerous software applications are being developed for the convenience of the citizens by Government of Punjab. For hosting these applications in a seamless manner, DGR and PSeGS needs a "Supplier" to provide cloud services and optionally, cloud managed services for hosting various software and applications of the Government of Punjab.

4.2. Invitation For Bid

4.2.1. Through this document, PSeGS invites tenders from reputed, experienced and financially sound Cloud Service Providers (CSP) having a valid MeitY, GoI empanelment or authorized partners of such CSPs to provide cloud services and optionally, cloud managed services to the Client for a range of hosting, storage as well as disaster recovery services etc. There will be no quantum of business obligation in respect of the cloud services to be taken by the Client from the Supplier either at present or in future.

4.2.2. The indicative quantity for the purpose of this RFP and discovery of rates is as below:

4.2.2.1. Windows based VMs:

Sl. No.	VM Configuration	VMs with Database			VMs with no database
		MS SQL	MySQL	PostgreSQL	
1.	1 Core, 2 GB RAM	-	-	-	5

2.	2 Core, 4 GB RAM	-	2	-	7
3.	2 Core, 8 GB RAM	-		1	3
4.	4 Core, 8 GB RAM	1	-	-	8
5.	4 Core, 16 GB RAM	1	1		3
6.	4 Core, 30 GB RAM	-	-	-	2
7.	8 Core, 16 GB RAM	-	-	-	5
8.	8 Core, 32 GB RAM	1	1		6
9.	16 Core, 56 GB RAM	21	-	-	0

4.2.2.2. Linux (CentOS / RHEL) based VMs:

Sl. No.	VM Configuration	VMs with Database			VMs with no database
		MySQL	Mongodb	PostgreSQL	
1.	1 Core, 2 GB RAM	-	-	-	7
2.	2 Core, 4 GB RAM	3	-	2	0
3.	2 Core, 8 GB RAM	2	1	2	1
4.	4 Core, 8 GB RAM	1	-	-	2
5.	4 Core, 16 GB RAM	2	-	1	3
6.	4 Core, 30 GB RAM	-	-	-	1
7.	8 Core, 16 GB RAM	-	-	2	4
8.	8 Core, 32 GB RAM	-	-	1	0
9.	16 Core, 32 GB RAM	-	-	-	3

4.2.2.3. Approx. total storage: 150 TB.

4.2.3. The maximum value of cumulative orders that can be placed through this RFP and contract thereof, is upto 50% more than the indicative order value (based on indicative quantity mentioned above). Purely for the purpose of calculating the indicative order value, the lowest price quoted by any of the bidder against each line item will be added.

4.2.4. The Client is free to take any of the services as listed in Financial bid and will not be limited to the indicative services listed above.

4.2.5. The prices discovered through this RFP may be used by PSeGS and /or other Departments / organizations of Government of Punjab.

4.2.6. Only the bidder, in whose name this tender document is purchased, shall be eligible to submit the bid.

4.2.7. PSeGS may, at its own discretion, extend the date for submission of bids. In such case, all rights and obligations of the PSeGS and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

5. Instructions to Bidders

5.1. General

5.1.1. All information supplied by bidders shall be treated as contractually binding on the bidders on successful award of the assignment by PSeGS on the basis of this tender.

5.1.2. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the PSeGS. PSeGS may cancel this RFP at any time prior to a formal written contract being executed by or on behalf of PSeGS.

5.1.3. This RFP does not constitute an offer by PSeGS. The bidder's participation in this process may result in PSeGS selecting the bidder to engage towards execution of the contract.

1.1.1

5.2. Validity of Bids

5.2.1. Bids shall remain valid till 180 (one hundred and eighty) days from the date of submission of bids. PSeGS reserves the right to reject a proposal valid for a shorter period as non-responsive.

5.2.2. In exceptional circumstances, PSeGS may solicit the bidder's consent to extend the period of validity. The request and the response thereto shall be made in writing. Extension of validity period by the bidder should be unconditional. A bidder may refuse the request without forfeiting the Earnest Money Deposit. A bidder granting the request will not be permitted to modify its Bid.

5.2.3. PSeGS reserves the right to annul the tender process, or to accept or reject any or all the bids in whole or part at any time without assigning any reasons and without incurring any liability to the affected bidder(s) or any obligation to inform the affected bidder(s) of the grounds for such decision.

5.3. Tender Document Fees

The bidder may download the tender document from the website as mentioned in document control sheet. The bidder shall furnish tender document fees, as part of the Eligibility Criteria, as per detail provided in the Document Control sheet.

5.4. Amendment to the Tender Document

5.4.1. Amendments necessitated due to any reasons, shall be made available on website only as provided in the document control sheet. It shall be the responsibility of the bidders to keep on visiting the website to amend their bids incorporating the amendments so communicated through the website. PSeGS shall not be responsible for any oversight or negligence on part of the bidders on the amendments to the terms and conditions of the tender document and notified through the website.

5.4.2. The corrigendum (if any) & any other related communication regarding this tender shall be posted only on the website and no separate communication either in writing or through email will be made to any interested/ participating bidders.

5.4.3. Any such corrigendum(s) or addendum(s) or clarification(s) shall be deemed to be incorporated into the tender document.

5.4.4. In order to provide prospective bidders reasonable time for taking the corrigendum(s) or addendum(s) into account, PSeGS, at its discretion, may extend the last date for the receipt of Bids.

5.5. Clarifications on submitted bids

During process of evaluation of the Bids, PSeGS may, at its discretion, ask Bidders for clarifications on their bids. The Bidders are required to respond within the prescribed time frame given for submission of such clarification.

5.6. Earnest Money Deposit (EMD)

5.6.1. The bidder shall furnish EMD, as part of the Eligibility Criteria, as per detail provided in the Document Control sheet.

5.6.2. The EMD shall be in Indian Rupees and bidder has to be paid through online mode.

5.6.3. EMD of the successful bidder will be released after the successful bidder signs the final agreement and furnishes the Performance Bank Guarantee (PBG) as performance security.

5.6.4. EMD of all unsuccessful bidders would be refunded by PSeGS as promptly as possible after signing of the agreement with the "Qualified and Responsive bidders".

5.6.5. The EMD submitted shall be interest free and will be refundable to the bidders without any accrued interest on it.

5.6.6. The Earnest Money will be forfeited on account of one or more of the following reasons:-

5.6.6.1. Bidder withdraws its bid during the validity period specified in the RFP.

5.6.6.2. Bidder does not respond to requests for clarification of its bid.

5.6.6.3. Bidder fails to provide required information during the evaluation process or is found to be non-responsive.

5.6.6.4. In case of a successful bidder, the said bidder fails to sign the Agreement in time; or furnish Performance Bank Guarantee in time.

5.6.6.5. The "Qualified and responsive bidder" fails to submit the Fixed Performance Security and / or fails to sign the contract after being intimated by PSeGS to do so.

5.7. Preparation of Bid

The Bidder must comply with the following instructions during the preparation of Bid:

5.7.1. The Bidder is expected & deemed to have carefully examined all the instructions, guidelines, forms, requirements, appendices and other information along with all terms and condition and other formats of the bid. Failure to furnish all the necessary information as required by the bid or submission of a proposal not substantially responsive to all the

requirements of the bid shall be at Bidder's own risk and may be liable for rejection.

5.7.2. The Bid and all associated correspondence shall be written in English and shall conform to prescribed formats. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Bidders. Any interlineations, erasures or over writings shall be valid only if they are authenticated by the authorized person signing the Bid.

5.7.3. The bid shall be uploaded on the www.eproc.punjab.gov.in website by the Bidder or duly authorized person(s) to bind the Bidder to the contract.

5.7.4. No bidder shall be allowed to modify, substitute, or withdraw the Bid after its submission.

5.7.5. The bidder shall be responsible for all costs incurred in connection with participation in the Bid process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of bid, in providing any additional information required by PSeGS to facilitate the evaluation process, in negotiating definitive "Qualified and Responsive bidders" and all such activities related to the bid process. PSeGS will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

5.7.6. Every page of the documents submitted by the bidder must be duly signed by the authorized signatory of the bidder along with the Organization seal.

5.7.7. The bids submitted by fax/e-mail etc. shall not be accepted. No correspondence will be entertained on this matter.

5.7.8. Failure to comply with the below requirements shall lead to the Bid rejection:-

5.7.8.1. Comply with all requirements as set out within this RFP.

5.7.8.2. Submission of the forms and other particulars as specified in this tender and respond to each element in the order as set out in this tender.

5.7.8.3. Non-submission of all supporting documentations specified in this RFP, corrigendum or any addendum issued.

5.8. Disqualifications

5.8.1. PSeGS may at its sole discretion and at any time during the evaluation of Bids, disqualify any Bidder, if the Bidder has:

5.8.1.1. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;

5.8.1.2. Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years.

5.8.1.3. Failed to provide clarifications related thereto, when sought;

5.8.1.4. Submitted more than one Bid (directly/in-directly);

5.8.1.5. Declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices or blacklisted.

5.8.1.6. Submitted a bid with price adjustment/variation provision.

5.8.1.7. Documents are not submitted as specified in the RFP document.

5.8.1.8. Suppressed any details related to bid.

5.8.1.9. Submitted incomplete information, subjective, conditional offers and partial offers submitted

5.8.1.10. Not submitted documents as requested in the checklist

5.8.1.11. Submitted bid with lesser validity period

5.8.1.12. Any non-adherence/non-compliance to applicable RFP content

5.9. Deviations

Bids submitted with any deviations to the contents of the Tender Document will be considered as non-responsive. No deviation(s) / assumption(s) / recommendation(s) shall be allowed with the bid. Bidders must ensure that pre-

bid meeting is attended by their concerned senior people so that all clarifications and assumptions are resolved before bid submission

5.10. Clarification on Tender Document

The bidders requiring any clarification on the bid document may submit his queries by the due date and time as mentioned in the Document Control Sheet in the following format in a MS Excel file:

Sl.No.	Page No.	RFP Clause No.	Clarification Sought
1.			
2.			

5.11. Bid Opening and Evaluation

5.11.1. PSeGS will constitute a committee to evaluate the Bids submitted by Bidders. A two-stage process, as explained hereinafter, will be adopted for evaluation of Bids. No correspondence will be entertained outside the process of evaluation with the Committee.

5.11.2. The Bids submitted will be opened at time & date as specified in the document control sheet by Committee or any other officer authorized by Committee, in the presence of bidders or their representatives who may wish to be present at the time of bid opening.

5.11.3. Only two persons for each participating bidder's shall be allowed to attend the Bid opening meetings.

5.11.4. The representatives of the bidders are advised to carry the identity card or a letter of authority from the bidders to establish their identity for attending the bid opening.

5.11.5. Committee may, at its discretion, call for additional information from the bidder(s) through email/fax/telephone/meeting or any other mode of communication. Such information has to be supplied within the set out time frame as provided by Committee, otherwise Committee shall make its own reasonable assumptions at the total risk and cost of the bidder and the bid may lead to rejection. Seeking clarifications cannot be

treated as acceptance of the bid. For verification of information submitted by the bidders, the committee may visit bidder's offices at its own cost. The bidders shall provide all the necessary documents, samples and reference information as desired by the committee.

5.12. Bid Evaluation

5.12.1. The bid evaluation will be carried out in a three stage process as under:

5.12.1.1. Pre-qualification / eligibility evaluation.

5.12.1.2. Technical evaluation.

5.12.1.3. Commercial bids evaluation.

5.13. Pre-qualfication / Eligibility Evaluation

5.13.1. The evaluation of the bidders will be carried out by the Committee as per the pre-qualification / eligibility criteria defined in the tender document. Only the bidders who fulfill the given pre-qualification / eligibility Criteria shall be eligible for next round of evaluation i.e. Technical evaluation. Non-conforming bids will be rejected and will not be eligible for any further processing.

5.13.2. The bidder can be a CSP or an authorized partner of the CSP. In case of an authorized partner, the CSP can authorize any number of bidders for the purpose of this RFP.

5.13.3. The eligibility criteria in case the bidder is a CSP empanelled with MeitY or an authorized partner of a CSP empanelled with MeitY are given as below:-

Sl. No.	Particulars	Eligibility Criteria	Supporting documents
1.	Legal Entity	The bidder should be either: • A company registered under the Indian Companies Act, 2013 OR • A partnership firm registered under the Limited Liability Partnerships (LLP) Act,	a. Certificate of Incorporation / Certificate of Registration b. Memorandum and

Sl. No.	Particulars	Eligibility Criteria	Supporting documents
		2008 OR • A partnership firm registered under the Indian Partnership Act, 1932.	Articles of Association / Partnership deed.
2.	MeitY empanelment as CSP	The bidder or the CSP of which the bidder is an authorized partner should be empanelled with MeitY for providing cloud services.	Self-certified copy of MeitY, GoI empanelment as CSP.
3.	Past Relevant Experience / Business Continuity	The bidder must have executed "Similar Work" order for at least 2 government / semi-government entities / reputed private organizations worth more than Rs. 200 crore in India from India in the last 3 years as on 31.08.2018. Minimum duration of each such "Similar Work" should be 6 months.	Work order / completion certificate or any other relevant proof should be submitted. Ongoing work order shall also be considered provided the work order is at least 6 months old as on 31.08.2018.
4.	Turnover	The bidder should have minimum annual average turnover of Rs. 5 crores from "Similar Work" only, in the last three financial years for which bidder's accounts have been audited. In case CSP is bidding directly, this clause is not applicable.	Certificate from statutory auditors / chartered accountant / published financial document clearly certifying the turnover requirements from "Similar Work"
5.	ISO Certification	The bidder should be ISO 9001:2008 or ISO 9001:2015 certified.	Self-certified copy of certification which is valid on date of bid submission.
6.	Capability to fulfil Scope of Work	The bidder or the CSP must have requisite capability to fulfil "Scope of Work" (on its own or through CSP) as laid out in Clause 5 of this RFP	Self-certified undertaking.
7.	Disclosures	The bidder shall submit the undertaking that their entity :- a. Has not been under a declaration of ineligibility for corrupt or fraudulent practices and should not be blacklisted by any State Govt. / Central Govt. / Board, Corporations and Government Societies / PSU for any	Self-Certified letter

Sl. No.	Particulars	Eligibility Criteria	Supporting documents
		reason. b. Has not been insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by court or judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons. c. And their directors, partners and officers not have been convicted of any criminal offense related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a cloud services supplying contract within a period of three years preceding the floating of this RFP, or not have been otherwise disqualified pursuant to debarment proceedings.	
8.	GST and PAN Registration	The Bidder should have valid GST registration certificate and PAN in the name of entity.	Self-certified copy of relevant valid certificates
9.	Furnishing RFP document fees and EMD	The bidder must ensure to deposit the tender document fees and EMD	Any relevant proof
10.	SLA compliance / mapping	The bidder shall provide a mapping of the service levels (objectives & targets) relevant for cloud services in the RFP to the current service levels offered by the CSP. Under no circumstances shall the current service levels offered be degraded than those indicated in this RFP.	Self-certified letter

Note: All the above mentioned documents have to be scanned and uploaded.

5.13.4. If the bidder is an authorized partner of a CSP empanelled with MeitY, the eligibility criteria shall provide an Authorization Certificate from a MeitY

empannelled CSP which states clearly that the bidder has been authorized to participate in this bid.

5.14. Technical Evaluation

5.14.1. The evaluation of the bidders will be carried out by the Committee as per the Technical Evaluation criteria defined in the RFP document. Only the bidders who qualify in the technical evaluation round shall be eligible for next round of evaluation i.e. Commercial Bid Opening. Bids of the bidders, who do not qualify in the technical evaluations stage, will be rejected and will not be eligible for any further processing.

5.14.2. The technical evaluation of the bidders shall be done based on the following parameters:

Sl. No.	Evaluation Criteria	Max. Marks
1.	Average Annual Turnover from "Similar Work" only, in the last two financial years for which bidder's accounts have been audited: Rs. 5 crore or more but less than Rs. 10 crore – 5 marks Rs. 10 crore or more but less than Rs. 15 crore – 7 marks Rs. 15 crore or more – 10 marks	10
2.	Years of operation in "Similar Work" only, as on 31.08.2018: 1 year or more but less than 2 years – 0 marks 2 years or more but less than 3 years – 5 marks 3 years or more – 10 marks	10
3.	Number of "Similar Work" handled (Minimum duration of each such "Similar Work" should be 6 months): Two "Similar Works" – 3 marks Three "Similar Works" - 7 marks Four "Similar Works" or more – 10 marks	10
4.	Out of "Similar Works" mentioned at Sl. No. 3, number of "Similar Works" done for a government entity: Zero "Similar Work" – 0 marks	10

Sl. No.	Evaluation Criteria	Max. Marks
	One “Similar Work” - 5 marks Two “Similar Works” or more – 10 marks	
5.	Number of Data Centers in India from where the MeitY empanelled Cloud Services are offered (The data centers should be in distinct physical locations and cannot be in adjacent facilities / buildings) One location – 0 marks Two locations – 5 marks Three locations or more – 10 marks	10
6.	Technical presentation of 15 minutes duration covering the bidder’s profile, CSP’s profile (in case of Partner of a CSP), experience in “Similar Work”, proposed architecture and features of Cloud Services as per scenarios mentioned in “Annexure-B: Capabilities requirement for Cloud Services” and ease of use.	10
7.	Evaluation of various features of Cloud Services w.r.t ease of use, as per the eight scenarios mentioned in “Annexure-B: Capabilities requirement for Cloud Services”. The bidder would be required to provide a demo login to the technical team of PSeGS with enough credit to evaluate the features. The bidder would be required to provide all possible technical / administrative support during this evaluation. (5 marks for each of the eight scenarios)	5 * 8 = 40

5.14.3. Ease of using the cloud services would be given higher importance while evaluating the technical presentation and demonstration.

5.14.4. Only those bidders who secure a Technical Score of 60% or more shall be considered for opening and evaluation of their Commercial bid.

5.15. Commercial Bids Evaluation

5.15.1. Commercial bids would be opened only for those Bidders, who secure the qualifying marks in the Technical Evaluation as explained above, on the prescribed date in the presence of bidder's representatives.

5.15.2. The bidders are free to quote rate of any or all the items. The rates quoted by such bidders shall help in identification of rates which will be used to arrive at L1 whenever a particular requirement (consisting of one or more items listed in the financial bid) of cloud services arises for the Client.

5.15.3. A contract will be signed with each "Qualified and Responsive bidder" which will be based on the rates identified in the financial bid (subject to downward revision by the "Qualified and Responsive bidders" from time to time).

5.15.4. Failure to abide the RFP conditions may result into forfeiture of EMD & PBG.

5.15.5. Any conditional commercial bid will lead to disqualification of the entire bid and forfeiture of the EMD.

5.15.6. Bidder quoting negative rates will be treated as non-responsive and will result in forfeiture of the EMD.

5.15.7. Errors & Rectification:

5.15.7.1. If there is a discrepancy between words and figures in the financial bid, the amount in figures will prevail.

5.15.7.2. If the bidder doesn't accept the correction of error(s) as specified, its bid will be rejected and EMD will be forfeited.

5.16. Notification of Award of Contract

PSeGS will notify the each "Qualified and Responsive bidders" in writing about acceptance of their bid. The notification of award will constitute the formation of the contract after submission of performance bank guarantee as mentioned in the clause 4.17.2 below as fixed performance security by the "Qualified and Responsive bidders".

5.17. Performance Security

5.17.1. The performance security is divided into two types – fixed and variable.

5.17.2. Fixed Performance Security:

5.17.2.1. As soon as possible, but not more than 15 days following receipt of letter of award of the contract, each "Qualified and Responsive bidder" shall furnish PBG of Rs. 5 lakh to PSeGS as "fixed" performance security. This is a one-time PBG only.

5.17.2.2. This PBG shall remain valid for a period of 180 (one hundred eighty) days beyond the expiry of the contract. Whenever the contract is extended, "Qualified and Responsive bidders" will have to extend the PBG proportionately.

5.17.2.3. In case a "Qualified and Responsive bidder" fails to submit this PBG within the time stipulated, PSeGS at its discretion may cancel the award of contract to that "Qualified and Responsive bidder"without giving any notice and the EMD of the concerned bidder will be forfeited.

5.17.3. Variable Performance Security

5.17.3.1. Whenever a work order is placed by the Client, the concerned Supplier would be required to submit a PBG with the concerned Client for an amount of 10% of the estimated value of each work order issued within 2 weeks of placing of order failing which appropriate action may be taken by PSeGS.

5.17.3.2. This PBG shall remain valid for a period of 180 (one hundred eighty) days beyond the expiry of the work order. Whenever the work order is extended, Supplier will have to extend this PBG proportionately.

5.17.3.3. In case the concerned "Supplier" fails to submit this PBG within the time stipulated, Client at its discretion may cancel the work order for the "Supplier" without giving any notice and invite the L2 bidder to supply the work order at L1 rates and submit the Variable Performance Security. The Fixed Performance Security of the L1 "Supplier" will be forfeited and will be required to submit a fresh Fixed Performance Security failing which the contract of such Supplier may be terminated.

5.17.4. The "Qualified and Responsive bidders" / Supplier(s) will not be entitled for any interest on the PBGs submitted.

5.17.5. The PSeGS and / or Client(s) shall forfeit their respective PBG (Fixed and / or Variable Performance Security) in full or part in the following cases:

5.17.5.1. When the terms and conditions of contract are breached/ infringed.

5.17.5.2. When contract is being terminated due to non-performance of the Supplier.

5.17.5.3. PSeGS incurs any loss due to "Supplier's" negligence in carrying out the project implementation as per the agreed terms & conditions.

5.17.5.4. If the Supplier fails to submit Variable Performance Security.

5.18. Signing of Contract

5.18.1. The "Qualified and Responsive bidders" will sign the contract with PSeGS within 15 working days of the release of notification and submission of fixed performance security.

5.18.2. While signing the contract and by 7th day of every quarter thereafter, the "Qualified and Responsive bidders" are required to submit publicly declared rates (for example, bidder's or it's CSP's website) in the same excel format as in the commercial bid. These rates will be purely used to keep track of upward / downward trends in the rates.

5.18.3. After signing of the contract, no variation in or modification of the terms of the contract shall be made except by mutual written amendment signed by both the parties.

5.19. Work orders

5.19.1. Whenever the Client needs the Cloud service, a requirement containing a list of line items (as identified in commercial bid) would be generated. Separate L1 would be identified for each such requirement of the Client. For each requirement, the prices quoted for the complete set of line items contained in the requirement will be taken to decide L1 bidder. If

for any item in the requirement, the "Qualified and Responsive bidders" has not quoted rates, such bidder will not be considered for L1 purpose.

5.19.2. An example of how L1 would be decided: Suppose, the Client needs a "Windows VM – 1 Core, 2 GB RAM" with 100 GB of "Premium Block Storage". For this requirement or item(s), the total cost of each of the "Qualified and Responsive bidder" will be calculated based on the prices identified in the financial bid. The "Qualified and Responsive bidder" offering lowest prices for the Client's requirement would be termed as L1 (Least Cost) bidder for that particular requirement. Similarly, L1 would be identified for each subsequent requirement of the Client. In case the cost for a particular requirement comes out to be same for two or more "Qualified and Responsive bidders", then the firm having higher total turnover for the financial year 2017-18 will be declared as the L1 bidder / Supplier for that particular requirement.

5.19.3. For a particular requirement, work order will be placed to only the L1 bidder, who, after submission of Performance Securities, would be known as the Supplier for that particular requirement. In case L1 bidder denies or is unable to fulfil the requirement, the Client reserves the right to obtain the services from the next lowest bidder.

5.19.4. Failure to provide services as per requirement by L1 bidder may result into forfeiture of EMD, PBG & termination of the contract.

5.19.5. The Client reserves the right to place a work order of any time duration.

5.19.6. The Client will intimate the Supplier in writing regarding any extension in the work order. Extension in the contract would not lead to extension of any of the in-force work orders.

5.19.7. Contract termination or expiry shall automatically lead to termination or expiry of all work orders which were issued based on the contract.

5.20. Fraud and Corrupt /Malpractices

All the Bidders must observe the highest standards of ethics during the process of selection of "Qualified and Responsive bidders" / Supplier(s) and during the performance and execution of contract.

5.20.1. For this purpose, definitions of the terms are set forth as follows:

5.20.1.1. **"Corrupt practice"** means the offering, giving, receiving or soliciting of anything of value to influence the action of the PSeGS or its personnel in contract executions.

5.20.1.2. **"Fraudulent practice"** means a misrepresentation of facts, in order to influence a selection process or the execution of a contract, and includes collusive practice among bidders (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non-competitive levels and to deprive PSeGS of the benefits of free and open competition.

5.20.1.3. **"Unfair trade practice"** means supply of services different from what is ordered on, or change in the Scope of Work.

5.20.1.4. **"Coercive practice"** means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the selection process or execution of contract.

5.20.2. PSeGS will reject a proposal for award, if it determines that the Bidder recommended for award, has been determined to having been engaged in corrupt, fraudulent or unfair trade practices.

5.20.3. PSeGS will declare a bidder ineligible, either indefinitely or for a stated period of time, for award of contract, if bidder is found to be engaged in corrupt, fraudulent and unfair trade practice in competing for, or in executing, the contract at any point of time.

6. Scope of Work

6.1.1. The Supplier shall be responsible for providing the required cloud services and optionally, cloud managed services as per the work order placed by the Client(s) as per the prices discovered through this RFP or as revised downward from time to time.

6.1.2. Supplier shall provide inter-operability 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.

6.1.3. The proposed application cloud environment should provide flexibility to scale the environment horizontally by adding more Virtual Machines of the same configuration to a load balanced pool. It should be possible to scale the solution horizontally at any time, without prior notification to the Supplier or its CSP. It should be possible to automate this process of scaling up and down automatically.

6.1.4. It should be possible at any time to move the Cloud Virtual Machines to PSeGS Data Center running industry leading Hyper Visors. The mechanism and technical requirements for achieving this should be well documented.

6.1.5. The CSP / Supplier should provide all variants of cloud service – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

6.1.6. The Supplier must provide the complete services within 24 hours of placing of work order.

6.1.7. The Supplier is required to have IP v6 support.

6.1.8. The billing would be done based on the duration for which the resources are active i.e. the Client only pays for the resources that are consumed. No charges would be levied by the Supplier when the resources are inactive.

6.1.9. There should be minimum 99.5% up time measured monthly for availability of the virtual machines and related services at the respective Data Center site.

6.1.10. The Supplier would be required to create and maintain a Helpdesk / telephonic number and email based ticketing system that will resolve problems and answer queries related to the work order. The help desk support to users shall be provided on 24 x 7 x 365 basis over telephone, chat and ticketing system.

6.1.11. The Supplier must submit a copy of work orders (and any amendments) issued by other user departments to PSeGS by 3rd working day of each month or earlier.

6.1.12. All terms and conditions of the CSP's empanelment with MeitY are automatically applicable to this RFP and contract thereof.

6.1.13. DR site should not be in the same premises as DC site. Both DR and DC sites should lie within India.

6.1.14. The SLAs and Penalties would be applicable as per "Annexure C: SLA and Penalties" at clause 7.7.

6.1.15. The bidder (on its own or through its CSP) must provide / offer the following capabilities:

6.1.15.1. Per second billing.

6.1.15.2. Freedom to adopt new Platforms and / or upgrade of existing platforms in an uncomplicated manner.

6.1.15.3. Hybrid Cloud.

6.1.15.4. Automatic software updates.

6.1.15.5. Virtually unlimited storage with option to increase storage in real time without human intervention of the bidder or CSP.

6.1.15.6. Containers as a managed service.

6.1.15.7. Active Directory.

6.1.15.8. Infrastructure as Code including post deployment scripting, service start-up and shut-down [based on tagging framework], etc.

6.1.15.9. Multiple Availability zones.

6.1.15.10. RESTful APIs for data access.

6.1.15.11. Metered pricing for capacity, data transfer and/or requests at a granular level (for example, per gigabyte per month for storage, per gigabyte transfer per month for bandwidth, etc).

6.1.15.12. Object-based cloud storage offering in general availability.

6.1.15.13. Software-defined compute, storage and networking, with access to a web services API for these capabilities.

6.1.15.14. Cloud software infrastructure services facilitating automated management, including, at minimum, monitoring, autoscaling services and database services.

6.1.15.15. A distributed, continuously available control panel supporting a hyperscale architecture.

6.1.15.16. Real-time provisioning for compute instances (small VM in five minutes) and a container service that can provision Docker containers in seconds.

6.1.15.17. An allowable VM size of at least 32 vCPUs and 244GB of RAM.

6.1.15.18. An allowable storage size of 1000 TB.

6.1.15.19. The ability to securely extend the customer's data center network into the cloud environment.

6.1.15.20. The ability to support multiple users and API keys, with role-based access control.

6.1.16. The Data Center facility (or each of the facilities where the cloud service offerings are proposed to be offered) must meet the following criteria:

6.1.16.1. The facility must be within India, should be currently operational and have a minimum capacity of 250 racks deployed only for cloud services.

6.1.16.2. Cloud platform should be certified for the latest version of ISO 27001 (year 2013), ISO 27017 & ISO 27018, by a competent auditing authority.

6.1.16.3. Cloud platform should be certified for Payment Card Industry Data Security Standards Level 1 version 3.2.

6.1.16.4. Cloud services should be audited for SOC – 1, 2 & 3.

6.1.16.5. Reports of periodic third party inspections/audits and the certifications should be available online or shared on demand for scrutiny.

6.1.16.6. The Supplier should provide the marketplace where the department can pick up 1st party & 3rd party applications for ready deployment.

6.1.16.7. The Supplier should offer Self Service Provisioning capabilities where there are near zero dependencies on the CSP.

6.1.17. In case the Supplier chooses to offer the cloud services proposed for accreditation from multiple data center facilities, each of the data center facilities shall meet the criteria.

6.1.18. The Supplier should offer a self-service portal which allows the client's IT admins to do the following activities without human intervention of CSP:

6.1.18.1. Provision of infrastructure services in near-real time.

6.1.18.2. Set rules for auto scaling of infrastructure.

6.1.18.3. Auto-scaling the infrastructure in near-real time, any number of times during a day.

6.1.19. For all the cloud services being quoted, the bidder has to ensure that all software being offered are genuine and comply to the licensing policy of the software OEM.

6.2. Scale-up and scale-down of resources

6.2.1. Due care would be taken by the Client in deciding the resources and services needed for every requirement. However, the need for increasing or decreasing the resources and services cannot be ruled out. Accordingly, the Client(s) may scale-down the resources or scale-up the resources as per their requirement, subject to below mentioned clauses.

6.2.2. All resources can be scaled up or down without any restrictions. The charges for replaced resource would be paid till they have been used. Similarly, the charges for additional resources would also be payable from the time they are put into service as per the rates provided by the Supplier or as revised from time to time.

6.2.3. For example, if the Client has taken a “Windows VM – 2 Core, 4 GB RAM” and 100GB of “Premium Block Storage (SSD)”, then if the Client desires to:

6.2.3.1. Scale down to “Windows VM – 1 Core, 2 GB RAM” and 50GB of “Premium Block Storage (SSD)” after 3 months of using the initially ordered resources, then charges for “Windows VM – 1 Core, 2 GB RAM” and 50GB of “Premium Block Storage (SSD)” shall be applicable immediately from the time when they are put into active mode and the billing for replaced resources shall be stopped immediately from the time they are replaced.

6.2.3.2. Scale up to “Windows VM – 4 Core, 8 GB RAM” and 200GB of “Premium Block Storage (SSD)” after 3 months of using the initially ordered resources, then charges for “Windows VM – 4 Core, 8 GB RAM” and 200GB of “Premium Block Storage (SSD)” shall be applicable immediately from the time when they are put into active mode and the billing for replaced resources shall be stopped immediately from the time they are replaced.

6.2.4. An amendment to the work order shall be issued by the Client whenever scale-down or scale-up (including auto scaling) of resources takes place.

6.2.5. The invoices by the Supplier should clearly indicate such scaling of resources.

6.2.6. The prices with the scaled-up or scaled-down resources would be reflected in all future invoices.

6.2.7. After scaling up or scaling down the resources, the resources and services would continue from the same Supplier to whom the initial order was placed. However, if the monthly order value of a particular work order is increased or decreased by more than 25% than the original monthly work order value, L1 bidder would be re-evaluated for that particular work order against the revised requirements. If this process results in a new L1 bidder, then the resources and services may be shifted to the new L1 bidder by terminating the work order with the current Supplier using the Clause 6.10.5 (Termination of work order due to increase or decrease in order value by more than defined limit).

6.3. Role of CSP, Supplier and Client

6.3.1. CSPs offer tools and services to help Clients meet their compute/storage requirements and security objectives. Suppliers (in case of managed services) and / or Clients are responsible for provisioning, configuration management, monitoring performance, governance & compliance and resource optimization using the breadth of services provided by the CSP.

6.3.2. Migrating to cloud creates a model of shared responsibility between the Client, Supplier and the CSP. The operations and maintenance of the infrastructure including host operating system and virtualization layer down to the physical security of the facilities in which the service operates will be the responsibility of the CSP. The Supplier and / or the Client has the responsibility for the management of the guest operating system (including updates and security patches), other associated application software, and the configuration and management of the security solutions provided by CSP such as security groups, host-based firewalls, host-based intrusion detection/prevention, encryption, and key management solutions. Deployment on cloud requires continuous monitoring and management by the Supplier.

6.3.3. In case the Client does not have skilled resources or expertise to migrate to cloud or manage the provisioned environment, the Client can procure Migration Services and/or Cloud Managed Services (e.g., provisioning, security configuration, monitoring) and / or Exit Management Services from the Supplier.

6.3.4. However, even if the Client procures Cloud Managed Services from the Supplier, in view of the shared responsibility, it is essential that the Client:

6.3.4.1. Monitors the operational activities to have the complete view into the provisioned cloud services and their configurations.

6.3.4.2. Review and validate the security configurations, review the notifications and patches released by the CSP.

6.3.4.3. Have the visibility into the provisioned infrastructure (including the utilizations) so that there is no over-provisioning leading to excess payments to the Supplier.

6.3.5. The Supplier in consultation with the Client will strive to optimize the provisioned resources by understanding the usage patterns and recommending termination of the under-utilized instances through continuous optimization. The Supplier / CSP is required to give timely suggestions for achieving such optimizations.

6.3.6. The Client may also discuss the possibilities of application re-engineering using advanced cloud features (e.g., auto-scaling, content delivery network) and additional PaaS services where possible to get further cost optimizations (e.g., Move large blob object and media files to Object storage and store a pointer in your existing database; migrate archival data to cold storage, etc)

6.4. Cloud Services

6.4.1. The Supplier has to provide access to the required cloud services for the Client to provision, migrate their workloads, configure security and manage the end-to-end operations.

6.4.2. The Supplier shall share the best practices with the Client with respect to architecture for resource optimization, high availability, security, reliability and reducing the risk of data loss / corruption.

6.5. Disaster Recovery Services

The supplier shall provide business continuity and disaster recovery services to meet the RPO and RTO as per the service levels. In case the primary environment goes down, the Supplier shall scale up the DR environment for the services to be delivered without any effect on the performance.

6.6. Migration Services

6.6.1. Migration Services are not a part of Cloud Managed Services (Refer Clause 5.7) and will have to be taken separately even if Cloud Managed Services have been opted. If the Client does not have expertise to

migrate their existing applications to Cloud, the Client can procure the cloud migration services from the Supplier which shall include the following:

6.6.2. Application and Infrastructure Discovery & Portfolio Analysis:

6.6.2.1. Formulate a baseline of the Client's technical environment including inventory of both applications and infrastructure. This should also include development/testing environments in addition to the production environment.

6.6.2.2. Document the technical details of the applications including technical architecture, integration with external solutions, underlying technologies / platforms, and underlying software. For each of the applications, capture the logical and physical deployment architecture providing the details of various architectural components (e.g., load balancer, firewall).

6.6.2.3. Identify the applications and their dependencies on other components and services. Create a dependency tree that highlights all the different parts of the applications and identify their upward and downstream dependencies to other applications.

6.6.3. Define TO BE and Security Architecture for Cloud

6.6.3.1. Estimate the resources required on cloud based on the application, current / anticipated server, storage configurations and workloads.

6.6.3.2. Define the indicative or the minimum requirements need to be provided for each kind of environment (Development, QA, Training, Staging, and Production - as applicable for the project) that is planned on cloud.

6.6.3.3. Supplier should propose and, in consultation with the department, finalize the security architecture for the workloads being migrated to cloud.

6.6.3.4. Define the logical architecture indicating the different compute, storage, network, security and monitoring services that will be provisioned for deploying the application on cloud.

6.7. Cloud Managed Services

6.7.1. In case the Client, does not have capacity to manage the provisioned cloud services, the Client can procure the cloud managed services (e.g., provisioning, security configuration, monitoring) from the Supplier.

6.7.2. These services exclude Migration Services and Exit Management Services, which need to be procured separately by the Client.

6.7.3. The scope of Cloud Managed Services includes the following:-

6.7.3.1. **Resource Management:** Adequately size the necessary compute, storage and other cloud services required, building the redundancy into the architecture and load balancing to meet the service levels. Based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute and storage as per the performance requirements of the solution. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by Department.

6.7.3.2. **Patch & Configuration Management (Remote OS Administration):** Manage the instances of compute, storage, and network environments. This includes department-owned & installed operating systems and other system software deployed by the Supplier.

6.7.3.3. **User Administration:** Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. Implement multi-factor authentication (MFA).

6.7.3.4. **Security Administration:** Configure, monitor and regularly review the security services / configurations for the workloads deployed on Cloud. Monitor the environment for unauthorized activity / access to the systems and conduct regular vulnerability scanning and penetration testing of the systems.

6.7.3.5. **Monitoring Performance and Service Levels:** Provide and implement tools and processes for monitoring the availability of assigned

applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.

6.7.3.6. **Backup (if procured by the Client):** Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by Client. Restore from the backup where required.

6.7.3.7. **Training:** Provide training to the officials of the Client on request. The training may be provided online or offline as per the requirements of the Client. The infrastructure for the offline training will be provided by the Client.

6.7.3.8. **Support for third party audits:** Enable the logs and monitoring as required to support for third party audits.

6.7.3.9. **Miscellaneous:** Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

6.7.3.10. **Provide the regular reporting to the Client:** Security assessment report with respect to security configuration gaps and possible improvements to the security and compliance of cloud services on a quarterly basis. In case any gaps / scope for improvement are identified, the same needs to be discussed with the Client and resolved in mutual consultation with the Client, either as fixed and hence no longer a gap or acceptable risk and hence no further action required.

6.8. Exit Management Services

6.8.1. These services are relevant at the end of the contract duration or in case of any mid-way termination of the contract or work order.

6.8.2. Exit Management Services is not a part of Cloud Managed Services (Refer Clause 5.7) and will have to be taken separately even if Cloud Managed

Services have been opted. But if the Client does not have expertise in migrate their existing hosted applications from the cloud provided by the Supplier to another cloud or another facility as deemed fit by the Client, the Client can procure the Exit Management Service from the Supplier which shall include the following:

6.8.3. The Supplier shall provide necessary handholding support (for a maximum of 60 days) to assist in transition of the services from the Supplier to Client or a replacement Supplier. The handholding support includes migration of the Virtual Machines, data, content and any other assets to the new environment created by the Client or any Agency (on behalf of Client) on alternate Supplier's offerings to enable successful deployment and running of the applications / websites on the new infrastructure.

7. General Contract Conditions

7.1. Standards of Performance

The Supplier(s) shall deliver the services and carry out their obligations under the contract with due diligence, efficiency and economy in accordance with generally accepted professional standards and practices. The Supplier shall always act in respect of any matter relating to this contract as faithful supplier to the Client. The Supplier shall always support and safeguard the legitimate interests of the Client, in any dealings with the third party. The Supplier shall conform to the standards laid down in the RFP in totality.

7.2. Contract Period

The contract signed with "Qualified and Responsive bidders" shall be valid for a period of 3 years from the date of signing of contract. If the services of the Suppliers are found satisfactory, contract may be extended for an additional period of maximum 2 years (1 year extension at a time) by mutual consent on the same terms & conditions.

7.3. Prices

7.3.1. The service charges quoted in the commercial bid shall be exclusive of all statutory duties & taxes.

7.3.2. The prices shall remain valid for the complete contractual period. No upward revision in prices will be accepted after opening of the bids and during the validity of the contract. However, the "Qualified and Responsive bidders" will pass on the benefit of any downward revision of the prices to the Client(s). Such downward revision in prices (or a better price offer by the Supplier) must be intimated to the Client(s) in the first week of each quarter. Such downward revision in prices shall be in proportion (or higher) to decrease in the publicly declared rates (for example, Supplier or its CSP's website) of the Supplier or its CSP. PSeGS will validate the downward revision of prices and notify the new prices by the 15th day of each quarter. The revised prices, once notified by

PSeGS, shall apply for all in-force and subsequent work orders. All invoices of in-force work orders too shall make immediate reference to the revised rates from the date on which the Supplier intimates the Client or PSeGS.

7.3.3. In case it comes to the notice of the Client that there has been a significant decrease in prices in the market, the Client may request the concerned "Qualified and Responsive bidder", even before the 3rd working day of the each quarter, to revise the prices accordingly.

7.3.4. After each downward revision of prices by any of the "Qualified and Responsive bidder", L1 bidder for the work orders already placed would not be re-evaluated. However, if the monthly order value of a particular work order is increased or decreased by more than 25% of the original monthly work order value due to the price revisions from time to time, L1 bidder would be re-evaluated for that particular work order. If this process results in a new L1 bidder, then the resources and services may be shifted to the new L1 bidder by terminating the work order with the current Supplier using the Clause 6.10.5 (Termination of work order due to increase or decrease in order value by more than defined limit).

7.3.5. Before 7th day of every quarter, the "Qualified and Responsive bidders" are required to submit their publicly declared rates (for example, Supplier or its CSP's website) in the same excel format as in the commercial bid. These rates will be purely used to keep track of upward / downward trends in the rates.

7.4. Additional Services

In case PSeGS determines that there are additional services that are being sought by the Clients, PSeGS may request all the Qualified and Responsive bidders to submit the pricing for such additional services during the validity of the contract on same terms and conditions.

7.5. Payment Terms

7.5.1. Payment to the Supplier shall be made in Indian Rupees through account payee cheque / NEFT / RTGS on monthly basis.

7.5.2. The invoices shall be raised only using GST No. of Punjab.

7.5.3. The invoices must be based on work orders (or any amendments thereof) issued by the Client(s).

7.5.4. The invoices must be based on resources actually consumed. No invoices shall be charged for inactive resources or for the duration when the resources were inactive.

7.5.5. The invoices should be separately generated for each work order for the particular payment period. The invoice should enclose the following:

7.5.5.1. Detailed usage report providing details of the consumption of the individual services during the payment period.

7.5.5.2. Detailed resource utilization report highlighting any under-utilization of resources with recommendations on how the resources can be optimized for the upcoming payment period.

7.5.5.3. SLA measurement report.

7.5.6. Applicable only when cloud managed services are procured: Security assessment report with respect to security configuration gaps and possible improvements to the security and compliance of applications deployed on cloud on a quarterly basis. The first report has to be submitted with the first month invoice and thereafter on a quarterly basis.

7.5.7. The payments will be made by the Client to the Supplier after verification of the invoice and SLA reports as early as possible.

7.5.8. Payments shall be subject to deductions / damages / penalties of any amount for which the Supplier is liable under the contract. Further, all payments shall be made subject to deduction of TDS (Tax Deduction at Source) at the rate applicable from time to time as per the Income-Tax Act, 1961 and any other applicable deductions/ taxes.

7.6. Applicable Law

Applicable Law means the laws and any other instruments having the force of law in India as may be issued and in force from time to time. The Contract shall be interpreted in accordance with the laws of the Union of India and the State of Punjab.

7.7. Governing Language

The Contract shall be written in English language. All correspondences and other documents pertaining to the contract, which are exchanged between the parties, shall be written in the English language.

7.8. Taxes and Duties

All taxes, duties and any statutory levies etc. payable by the Supplier during the contract tenure shall be the sole responsibility of the Supplier.

7.9. Data Ownership and Confidentiality

7.9.1. The concerned Client 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.

7.9.2. The concerned Client shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application.

7.9.3. The Supplier shall keep the data of the Clients strictly confidential, otherwise there may be financial and legal implications as per the prevalent law of Centre / State.

7.10. Termination of Contract or Work Orders

7.10.1. The contract or work orders can be terminated by the parties as detailed below. In such case, the provisions under Exit Management (Clause 6.11) shall apply.

7.10.2. Termination of contract shall automatically lead to termination of all work orders issued on the basis of contract.

7.10.3. **Termination of Work Order for default:** The Clients can terminate the work order in the event of default of terms and conditions of this RFP or the contract / work order by the Supplier by giving 2 months' written notice.

7.10.4. **Termination of Work Order for convenience:** The Client reserves the right to terminate, by prior written 2 months' notice, the whole or part of the contract, at any time for its convenience. The notice of termination shall specify that termination is for the Client's convenience, the extent to which performance of work under the work order is terminated, and the date upon which such termination becomes effective.

7.10.5. **Termination of work order due to increase or decrease in order value by more than defined limit:** The Client reserves the right to terminate, by prior written 2 months' notice, the whole of the work order, at any time due to increase or decrease in the monthly work order value of a particular work order by more than 25% of the original work order value. The notice of termination shall specify that termination is due to the aforesaid reason and the date upon which such termination becomes effective.

7.10.6. **Termination of Contract for default:** PSeGS or the "Qualified and Responsive bidders" / Supplier(s) can terminate the contract in the event of default of terms and conditions of this RFP or the contract by the other party by giving 2 months' written notice.

7.10.7. **Termination of contract for Insolvency, Dissolution, etc:** PSeGS may at any time terminate the Contract by giving written notice to the "Qualified and Responsive bidder(s)" / Supplier(s), if the concerned "Qualified and Responsive bidder" / Supplier becomes bankrupt or otherwise insolvent or in case of dissolution of firm/company or winding up of firm/company. In this event termination will be without compensation to the "Qualified and Responsive bidder" / Supplier,

provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to PSeGS.

7.10.8. Termination of contract for Convenience: PSeGS or the "Qualified and Responsive bidder(s)" / Supplier(s) reserves the right to terminate, by prior written 2 months' notice, the whole or part of the contract, at any time for its convenience. The notice of termination shall specify that termination is for the concerned party's convenience, the extent to which performance of work under the contract is terminated, and the date upon which such termination becomes effective.

7.11. Exit Management

7.11.1. The duration of Exit Management will normally be of 2 months from date of termination or two months prior to expiry of contract / work order. In case of providing services post termination or post expiry of the work order, the client will pay for the services consumed during the exit management period.

7.11.2. During the exit management period and for 30 days post expiry of the work order / contract, the Supplier will not take action to remove any Client content as a result of the termination or expiry of contract / work order. In addition, during such period, the Supplier will permit the Client or its nominated agency to access the cloud services for the Client to retrieve any remaining Customer Content, delete and purge all Customer Content from the cloud services. The Supplier shall also allow the Client access to information to enable Client to assess the existing services being delivered.

7.11.3. During the exit management period, the Supplier shall ensure supply of all services as per the work order so that the business of the Client is not affected.

7.11.4. The Supplier shall provide all such information as may reasonably be necessary to affect as seamless a handover as practicable in the circumstances to Client / replacement Agency and which the Supplier

has in its possession or control at any time during the exit management period.

7.11.5. All information (including but not limited to documents, records and agreements) in digital and/ or paper form relating to the services reasonably necessary to enable Client and its nominated agencies to carry out due diligence in order to transition the provision of the Services to Client or its nominated agencies, must be maintained by the Supplier from commencement of the services.

7.11.6. The Client will issue a written sign-off after the successful transition from the Supplier. Supplier shall not delete any content till such a written sign-off is provided by the Client along with an explicit request to delete the content.

7.11.7. The Supplier will be paid only for the services rendered until the services are being rendered by the Supplier. If the sign-off is provided before the exit management period is over, the applicable charges will only be paid until the sign-off.

7.11.8. The payment for the final month invoice along with any applicable exit management service costs will be paid only on the written sign-off from the Client.

7.12. Force Majeure

7.12.1. The Supplier shall not be liable for forfeiture of its PBG or termination of contract for default if and to the extent that delays in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

7.12.2. “Force Majeure” means an event beyond the control of the Supplier and not involving the Supplier’s fault or negligence, and unforeseeable. Such events may include, but are not restricted to, acts of wars or revolutions, riot or commotion, earthquake, fires, floods, epidemics, and quarantine restrictions.

7.12.3. If a Force Majeure situation arises, the Supplier shall promptly notify the Client(s) in writing of such condition and the cause thereof. Unless otherwise directed by the Client(s) in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

7.13. Resolution of Disputes

If any dispute arises between parties, then these would be resolved in following ways:

7.13.1. **Amicable Settlement:** Performance of the Contract is governed by the terms and conditions of the Contract, however at times dispute may arise about any interpretation of any term or condition of Contract including the scope of work, the clauses of payments etc. In such a situation either party of the contract may send a written notice of dispute to the other party. The party receiving the notice of dispute will consider the Notice and respond to it in writing within 30 days after receipt. If that party fails to respond within 30 days, or the dispute cannot be amicably settled within 60 days following the response of that party, then the second Sub-clause of resolution of disputes shall become applicable.

7.13.2. **Arbitration:** In case dispute arising between the parties, which has not been settled amicably, the “Qualified and Responsive bidder” / Supplier can request PSeGS to refer the dispute for Arbitration under Arbitration and Conciliation Act, 1996. Such disputes shall be referred to the Arbitrator which shall be “Vice Chairman-PSeGS”. The Indian Arbitration and Conciliation Act, 1996 and any statutory modification or re-enactment thereof, shall apply to these arbitration proceedings. Arbitration proceedings will be held at Chandigarh. The decision of the arbitrator shall be final and binding upon both the parties. All arbitration awards shall be in writing and shall state the reasons for the award. The

expenses of the arbitration as determined by the arbitrator shall be borne equally by PSeGS and the "Qualified and Responsive bidder" / Supplier. However, the expenses incurred by each party in connection with the preparation, presentation and litigation shall be borne by the party itself.

7.14. Legal Jurisdiction

All legal disputes between the parties shall be subject to the jurisdiction of the Courts situated in Chandigarh, India only.

8. Bid Formats

Following are the Bid formats to be used by the bidders for submitting their Bids online for selection as Supplier under the RFP:-

Sl. No.	Form	Description
1.	Form - 1	Covering Letter
2.	Form - 2	Eligibility Criteria Form
3.	Form - 3	CSP Compliance Form
4.	Form - 4	Commercial Bid Form

*[**Note:** Italicized comments in rectangular brackets of formats have been provided for the purpose of guidance/ instructions to bidders for preparation of the Proposal Formats. These should not appear in the final bids to be submitted by the bidders*]

8.1. Form-1: Covering Letter for participating in the bidding process

Bid Reference No. : PSeGS/Cloud/2018/1
[Bidders are required to submit the covering letter as given here on their letterhead]

To

Member Secretary,
Punjab State e-Governance Society,
O/o Department of Governance Reforms,
Plot D-241, Industrial Area, Phase 8B, Sector – 74, Near Quark City,
Mohali-160071

Sub: Bid for selection as Supplier of Cloud Services

Dear Sir,

1. We, the undersigned, have carefully examined the referred tender no. PSeGS/Cloud/2018/1, offer to propose for the selection as **Supplier of Cloud Services**, in full conformity with the said RFP.

2. We have read all the provisions of RFP & Corrigendum and confirm that these are acceptable to us.

3. We further declare that additional conditions, variations, if any, found in our proposal shall not be given effect to.

4. We agree to abide by this Bid, consisting of this letter and commercial bid, and all attachments, till 180 days from the date of submission of bids as stipulated in the tender and modifications resulting from contract negotiations, and it shall remain binding upon us and may be accepted by you at any time before the expiration of that period.

5. Until the formal final Contract is prepared and executed between us, this Bid, together with your written acceptance of the Bid and your notification of award, shall constitute a binding contract between us.

6. We hereby declare that all the information and statements made in this proposal are true and accept that any misrepresentation or misinterpretation contained in it may lead to our disqualification.

7. We understand you are not bound to accept any bid you receive, not to give reason for rejection of any bid and that you will not defray any expenses incurred by us in bidding.

8. We declare that this is our sole participation in this tender bid and we are not participating/co-participating through any of other related party or channel.

9. We have not been blacklisted or barred by any State Govt. / Central Govt. / Board, Corporations and Government Societies / PSU for any reason.

10. EMD of Amount Rs. 2 Lakh (Rs. 2,00,000/-) has been paid online. Details are as below:-
    [Insert the details as applicable].

11. RFP document cost has also been paid online. Details are as below:-
    [Insert the details as applicable].

12. Our details have been filled below:-

S.No	Particulars	Details
1.	Name of the Bidder	
2.	Name of CSP	
3.	Principal place of business:	
4.	Address with Telephone numbers, Fax number etc.	
5.	Date of incorporation and/or commencement of business	
6.	Name of Partners/ Directors	
7.	Registration Number	
8.	PAN Number	
9.	GST Registration Number	
10.	Brief description of the Bidder's line of business	
11.	Name, designation, postal address, e-mail address, phone numbers (including mobile) etc., of Authorized Signatory of the Bidder with power of attorney.	

12.	Details of individuals who will serve as the point of contact/communication with the PSeGS in case of the award of the contract. *[The details to include Name, designation, postal address, e-mail address, phone numbers (including mobile) etc.]*	

13. Details of supplying cloud related works/contracts that are in progress or have been completed (Proofs attached) :-

Sl. No.	**Name of the Client**	**Type of Work**	**Value of Contract (Rs.)**	**Contract start date**	**Contract completion date**

Signature

Full Name

In the capacity of

Duly authorised to sign Proposal for and on behalf of

Date…….. **Place……..**

[: Strike off whichever is not applicable]*

8.2. Form 2: Eligibility Criteria Form

Bid Reference No. : PSeGS/Cloud/2018/1

8.2.1. The compliance against each of the particulars provided under Clause 4.13.3 (In case the bidder is a CSP empanelled with MeitY or its authorized partner) is to be submitted as per below format:-

Sl. No.	Particulars	Eligibility Criteria	Supporting documents	Pg. No.	Compliance (Yes / No)
…	…	…	…	…	…

Note: All the above mentioned documents have to be scanned and uploaded.

8.3. Form 3: CSP Compliance Form

[To be submitted by the bidder as per the format provided below]

Capabilities listed under Clauses 5.1.15, 5.1.16 and 5.1.17	Compliance (Y/N)	Native Service or Compliance through a third party solution implementation (Native / Third Party)	In case of a native service, provide the CSP's service name through which such a capability is offered. In case of a third party solution, please provide the name of the third party solution	Public Website Link (public link for the native service) or (public link for the third party solution documentation)
…	…	…	…	…

Capabilities listed under Annexure B: Capabilities requirement for Cloud Services	Compliance (Y/N)	Native Service or Compliance through a third party solution implementation (Native / Third Party)	In case of a native service, provide the CSP's service name through which such a capability is offered. In case of a third party solution, please provide the name of the third party solution	Public Website Link (public link for the native service) or (public link for the third party solution documentation)
…	…	…	…	…

8.4. Form 4: Commercial Bid Form

[To be submitted by the bidder as per the format provided on the e-procurement website]

8.5. Annexure A: Performance Bank Guarantee

<Name>
<Designation>
<Address>
<Phone Nos.>
<Fax Nos.>
<Email id>

Whereas, <<name of the Supplier and address>> (hereinafter called "the applicant/Supplier") has undertaken, in pursuance of contract no. <<insert contract no.>> dated. <<insert date>> to provide consulting services for <<name of the assignment>> to <<PSeGS>> (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the applicant/Supplier shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, **<<Name of the Bank>>** a banking company incorporated and having its head /registered office at <<address of the registered office>> and having one of its office at <<address of the local office>> have agreed to give the Supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the Supplier, up to a total of **Rs. <<Insert Value>> (Rupees <<insert value in words>> only)** and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs**. <<Insert Value>>** (Rupees **<<insert value in words>>** only**)** as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the applicant/Supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Supplier shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until *<<Insert Date>>*.

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed **Rs <<Insert Value>> (Rupees <<insert value in words>> only).**
II. This bank guarantee shall be valid up to *<<insert expiry date>>*.
III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for

payment under this bank guarantee on or before *<<insert expiry date>>* failing which our liability under the guarantee will automatically cease.

8.6. Annexure B: Capabilities requirement for Cloud Services

8.6.1. **Scenario #1**: Self Provisioning (VMs of different configurations, Storage of different IOPS, etc.)

8.6.1.1. Ease of provisioning; agility, self-service, availability of different configurations of VMs and storage for self-provisioning

8.6.1.2. Availability of per second billing.

8.6.1.3. Demonstrate, at a high level, the CSPs console or publicly available offerings/resources:

8.6.1.3.1. Storage capabilities

8.6.1.3.2. Compute capabilities – Create a VM of 32 cores and 244 RAM (or higher)

8.6.1.3.3. Database capabilities and types

8.6.1.3.4. Networking

8.6.1.3.5. Management and Analytical tools

8.6.1.3.6. Security

8.6.1.3.7. Hybrid Cloud

8.6.1.3.8. Automatic software updates

8.6.1.3.9. Global speed of data

8.6.1.3.10. Active Directory

8.6.1.3.11. IaC (Infrastructure as Code)

8.6.1.3.12. RESTful APIs for data access.

8.6.1.3.13. Other capabilities.

8.6.1.4. Storage:

8.6.1.4.1. Storage options

8.6.1.4.2. Types of available storage (e.g.; block, object) and data life-cycle processes,

8.6.1.4.3. Establish a storage volume and evaluate how data is loaded and retrieved.

8.6.1.4.4. Create a 100 TB storage volume with and without a compute option. Option to extend the storage by 20 times in real time without human intervention of the CSP.

8.6.1.4.5. Validate permissions to access these volumes.

8.6.1.5. Demonstrate the ability to use multiple methods for interacting with the cloud computing services (e.g., Application Program Interface (API), web console, command line).

8.6.2. **Scenario #2:** Auto-scaling to 10X of compute resources in rela time without human intervention

8.6.2.1. Evaluate on ability to auto-scale; ease of configuring the auto-scaling rules, breadth of parameters for configuring auto-scaling (e.g., min/ max/parameters on which threshold levels can be set/wait time), availability of multiple auto-scaling scenarios (e.g., based on threshold levels, scheduled, recurring).

8.6.2.2. Demonstrate the scale of your offering by setting up large scale compute and storage solutions.

8.6.3. **Scenario #3**: Architecture to support High Availability and Business Continuity to meet the minimal RPO / RTO requirements.

8.6.3.1. Evaluate on architecture proposed to meet the High Availability and RPO / RTO requirements.

8.6.3.2. Evaluate on demonstration of load balancing features supporting multiple routing mechanisms including round-robin, failover, sticky session, etc.

8.6.3.3. Evaluate how you can create an environment in two or more separate isolated locations. Also, evaluate load balancing between these environments.

8.6.3.4. Multiple availability zones.

8.6.4. **Scenario #4**: Evaluation of security features from the CSP to support security of the application and data in the cloud

8.6.4.1. Cloud Security against attacks like DoS / DDoS attacks, DNS attacks, Perimeter security etc.: Evaluate on the availability of features such as Multi-factor authentication, Identity & Access Management, Private Subnets, Data Encryption – Client Side and Server Side Encryption, Web Application Firewall and DDoS to help protect web applications from common web attacks such as SQL injection or

cross-site scripting, Dedicated Network Connection using industry-standard 802.1q VLANs, and Centralized Key Management.

8.6.4.2. Demonstrate how virtual environments can be isolated from security and networking perspective:

8.6.4.2.1. Create subnets

8.6.4.2.2. Internet routing

8.6.4.3. How Identity and Access Management (IAM) can separate access to various resources:

8.6.4.3.1. How to secure an account?

8.6.4.3.2. Create users and groups

8.6.4.3.3. Attach policy

8.6.4.3.4. Set up passwords

8.6.4.3.5. Only the resource with appropriate permissions and grants has access to any specific resource

8.6.4.3.6. All access and changes carried out are logged, cannot be tampered with and be audit-able

8.6.4.4. Illustrate how an end user requests various services from cloud offerings. Demonstrate:

8.6.4.4.1. How accounts are established?

8.6.4.4.2. How security provisions are enabled?

8.6.4.4.3. How main accounts can be divided into sub accounts?

8.6.4.5. Accounts:

8.6.4.5.1. Describe the account key system (root and user) used in the demo.

8.6.4.5.2. Demonstrate how you manage and protect your account keys

8.6.4.6. Automated security assessment service to help improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices.

8.6.4.7. Showcase CSP's documentation around security operations of the platform and international best practices adopted by your Cloud Operations.

8.6.5. **Scenario #5**: Demonstration of the Cloud Governance Capabilities: Evaluate on the demonstration of features available to support Cloud Governance by Government Agency

8.6.5.1. Inventory of all resources provisioned in the Cloud along with their configuration attributes.

8.6.5.2. Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.

8.6.5.3. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.

8.6.5.4. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.

8.6.5.5. Capture logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.

8.6.5.6. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Agencies should be given the ability to dig into the configuration history to perform incident analysis.

8.6.5.7. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.

8.6.6. **Scenario #6**: Information Availability for the customer on the CSP Portal:

8.6.6.1. Published uptimes

8.6.6.2. Health dashboard of the overall cloud services

8.6.6.3. Health dashboard of the cloud services provisioned for the customer

8.6.6.4. Incident Reports

8.6.6.5. Security Bulletins

8.6.6.6. Audit Reports

8.6.6.7. Billing details

8.6.7. **Scenario #7**: Managed Platform Services

8.6.7.1. Automatic failover, backup & recovery, isolation & security, push-button scaling, automated patching, advanced monitoring, and routine maintenance are the responsibilities of the CSP. Project team should be able to do the following: application upgrades, schema design, query construction and query optimization.

8.6.7.1.1. Relational Database as a Service for MySQL, PostGreSQL, MS SQL

8.6.7.1.2. NoSQL Database

8.6.7.2. Data Warehouse

8.6.7.3. Caching Services

8.6.7.4. Container Services

8.6.8. **Scenario #8**: Self-Service and Automation Capabilities

8.6.8.1. Creating (provisioning and configuring) own network topology (firewalls, sub-nets, routing tables, network ACLs, private IP range, VPN gateways).

8.6.8.1.1. Self-configure load balancers – network & application

8.6.8.1.2. Automated scheduled backups

8.6.8.1.3. Deploy VMs in multiple security zones, as required for the project, defined by network isolation layers in the Customer's local network topology

8.6.8.1.4. Role Based Access Control to segregate users based on their roles and privileges

8.6.8.1.5. Set alarms on the metrics to receive near-real time notifications on any changes in the health of the services

8.6.8.1.6. Ability to take other automated actions when the metric crosses user-specified threshold

8.6.8.1.7. Provisioning of Virtual Machines

8.6.8.1.8. Provisioning of Block Storage

8.6.8.1.9. Provisioning of Object Storage

8.6.8.1.10. Storage Life-cycle management

8.6.8.1.11. Define auto-scaling rules on the administration console w/o any additional scripting

8.6.8.1.12. Dynamically adding / removing VMs from the load balancers based on the health check

8.6.8.1.13. Provision to re-allocate static public IP between Vms

8.6.8.1.14. Attaching additional block storage; deleting a storage volume; encryption; incremental backup; configure backup retention policy (e.g., automatically delete the backup after seven days)

8.6.8.1.15. Auto-scaling

8.6.8.1.16. Ability to create templates (e.g, describe the cloud resources, and any associated dependencies or runtime parameters, required to run your application) to deploy and update infrastructure as code

8.7. Annexure C: SLA and Penalties

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:

8.7.1. The SLA parameters shall be monitored on a monthly 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 Client, then the Client will have the right to take appropriate disciplinary actions including termination of the contract.

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

8.7.3. The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The Supplier shall make available the Monitoring tools for measuring and monitoring the SLAs. The Supplier 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 Client on a monthly basis. Client and PSeGS 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. PSeGS or Clients may audit the tool and the scripts on a regular basis.

8.7.4. The measurement methodology / criteria / logic will be reviewed by Client / PSeGS.

8.7.5. In case of default on any of the service level metric, the Supplier shall submit performance improvement plan along with the root cause analysis for the Client ’s approval.

8.7.6. In case these service levels cannot be achieved at service levels defined in the agreement, PSeGS shall invoke the performance related penalties. Payments to the Supplier will be linked to the compliance with the SLA metrics laid down in the agreement.

8.7.7. In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.

8.7.8. Penalties shall not exceed 100% of the monthly bill. If the penalties exceed more than 50% of the total monthly bill, it will result in a material breach. In case of a material breach, the Supplier will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the Client.

Sl. No.	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
Availability / Uptime				
1.	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, Load Balancer, Security Services,)	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) provisioned in the cloud. Measured with the help of SLA reports provided by the Supplier.	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resource will attract penalty as indicated below. • < 99.5% & >= 99% (10% of the <<Periodic Payment>>) • < 99% and >= 95% (30% of the <<Periodic Payment>>) • <95% (100% of the <<Periodic Payment>>)
2.	Availability of Critical Services (e.g. Register Support Request or Incident; Provisioning / De-	Availability will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs	Default on any one or more of the services on either of the portal or APIs will attract penalty

Sl. No.	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
	Provisioning; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)		(where applicable) >= 99.5%	as indicated below • < 99.5% and >= 99% (10% of the <<Periodic Payment>>) • < 99% (10% plus 2% of the <<Periodic Payment>> for each percentage drop below 99%)
3.	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the MeitY's Empanelment Requirements.		15 working days from the date of publishing of report. If STQC issues a certificate based on the audit then this SLA is not required.	5% of <<periodic Payment>>
4.	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		Along with monthly invoice	5% of <<periodic Payment>>
Support Channels – Incident and Helpdesk (as per Clause 5.1.10)				
5.	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 15 minutes	< 95% (1% of the <<Periodic Payment>> for each percentage drop below 95%)
6.	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 30 minutes of problem reporting	• < 98% & >= 90% (5% of the <<Periodic Payment>>) • < 90% & >= 85% (10% of the <<Periodic Payment>>) • < 85% (15% plus 1% of the <<Periodic Payment>> for each percentage drop below 85%)

Sl. No.	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
7.	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 AND 95% of Severity 3 within 16 hours of problem reporting	• < 95% & >= 90% (2% of the <<Periodic Payment>>) • < 90% & >= 85% (4% of the <<Periodic Payment>>) • < 85% (6% plus 1% of the <<Periodic Payment>> for each percentage drop below 85%)
Service Levels relevant when procuring DR services on Cloud:				
8.	Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <= 4 hours	For delay of each additional 2 hours, 0.5% (or part thereof) of the <<Periodic Payment>> shall be levied as additional liquidated damages.
9.	Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours	For delay of each additional 30 minutes, 0.5% (or part thereof) of the <<Periodic Payment>> shall be levied as additional liquidated damage

Note: Periodic Payment means monthly payment

8.7.9. Maximum cumulative penalty cannot exceed 10% of the work order value after which the Client may cancel the work order and forfeit the Variable Performance Security submitted by the Supplier. If for any Supplier, this cumulative penalty cap is hit twice against various work orders, then PSeGS will forfeit the Fixed Performance Security submitted by the Supplier and may also lead to termination of the contract.

8.7.10. Severity Levels

8.7.10.1. Below severity definition provide indicative scenarios for defining incidents severity. However PSeGS 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.	