Central Directorate of National Savings, Islamabad

Request for Proposal/Bidding Document

For

Provisioning of Managed Services and 24/7 NOC Operations for CDNS's Data Centers (PR & DR Sites)

Government of Pakistan

Ministry of Finance

www.savings.gov.pk

January, 2026

(SAY NO TO CORRUPTION)

Tender Notice

1. Central Directorate of National Savings (CDNS), invites electronic bids on PPRA e-Pak Acquisition & Disposal System (EPADS) for Provisioning of Managed Services and 24/7 NOC Operations for CDNS's Data Centers (PR & DR sites) from well reputed firms/companies/JVs/ consortium registered with taxation authorities and having their own well established offices and supervisory structure for the initial period of three years (further extendable for one year).

2. The detailed **Request for Proposals (RFPs)** which would be the integral part of this tender may be obtained from undersigned during office hours or can be downloaded from www.savings.gov.pk or www.ppra.org.pk

3. The Procurement Method as per PPRA Rule 36(b) [Single stage-Two Envelope Procedure] will be observed for this tender. Bidders are required to submit their bids through PPRA EPADS (www.eprocure.gov.pk) however, the bid security in original amounting to Rs. 1,000,000/- (rupees one million) in the shape of a Bank Draft/Pay Order/Demand Draft /CDR/Bankers Cheque/Cashier Cheque only, issued from any scheduled bank operating in Pakistan in the favour of "CDNS, Islamabad" must be submitted to CDNS in original on technical bid opening date and time, **without bid security. The proposal shall not be entertained/ accepted and be rejected straight away.** Bid must be submitted online through EPADS as per schedule i.e on **20-01-2026 up to 11:30 a.m**. Bids will be opened on the same day at **12:00 Noon** at Conference Room of Central Directorate of National Savings (CDNS), 23-N, Civic Centre, G-6 Markaz, Islamabad in the presence of the bidders or their representatives who wish to attend the proceedings.

4. The Procuring Agency reserves the right to reject any/all or a part of bids prior to the acceptance of a bid or proposal, for which reason(s) may be conveyed if desired in writing as per PPRA Rule-2004.

5. For any query related to this tender notice, please feel free to contact the undersigned.

Director (Operations)

Ph: 051-9215753

23-N, Savings House, Central Directorate of National Savings, Ministry of Finance, Civic Centre, G-6 Markaz, Islamabad

1. Introduction to Central Directorate of National Savings

1.1. Central Directorate of National Savings (CDNS) is an attached department of the Finance Division, with a vision to "promote and inculcate the value of thrift for mobilization of savings" and a mission to "be the preferred institution for small savers to facilitate objective of financial inclusion".

1.2. Following are the core objectives of the CDNS:

a) Inculcate the habit of thrift among masses.
b) Provide secure deposit avenues to small savers thus contributing towards the goal of financial inclusion.
c) Provide a safety net to special segments of society like widows, senior citizens (60 years and above) and retired government servants, disabled/special persons, families of martyr of armed forces, Law Enforcement Agencies and civilians who are victims of war on terrorism in the absence of effective social security system.
d) Channelize the un-conventional savings to the financial system.
e) Assist the government in policy formulation regarding savings.
f) Provide non-inflationary and non-bank borrowing to the government to bridge overall fiscal deficit (OFD).

1.3. CDNS is a premier financial institution offering retail government securities and savings products (known as National Savings Schemes (NSS), providing level playing field to small savers through diversified product mix. It is a key contributor towards financial inclusion with an investor base of around 2.9 Million and a portfolio of about PKR 3,400 billion, which is around 24% of total banking deposits. Its share in domestic debt of government is around 19%. Most of its products are designed for low-income segments of the society, however due to operational and IT constraints, it is unable to play its role to extend financial services to the low-income segments. Existing product mix of NSS are ranging from short-term to long-term in terms of tenor and for students, youth, widows, senior citizens and pensioners in terms of segments of society. At present, NSS are being offered through a network of 376 National Savings Centres (NSCs). Apart from offering NSS through National Savings Centers (NSCs), these are also being offered through agency arrangements with the network of selected commercial scheduled banks operating in Pakistan. Thus, outreach of NSS is in every nook and corner of the country.

1.4. It is apprised that CDNS is putting efforts for inculcating the habit of savings in general public. It also supports the 'National Financial Inclusion Strategy' and is gradually increasing the access of financial services for households and businesses, CDNS endeavors to improve the usage of digital financial services and payment systems in the country. It is also worth mentioning here that CDNS has recently taken several initiatives for revamping of CDNS business application software from distributed to centralized architecture. This includes offering Alternate Delivery Channels (ADCs), Biometrics, Automated Teller Machine (ATM) & Point of Sale (PoS) Cards and access to accounts through cell phones & web/ internet, Enterprise Resource Management (ERP) Systems through core banking system etc. Thus, substantial improvement in customer service, decreased employee workload, and extension of additional value-added facilities to the investors, and promotion of financial inclusion in the country. In order to establish the Digital Financial Services & Payment Systems ("DFS & PS") and technology based driven business operations, several national and multinational firms/organizations are facilitating CDNS in achieving its vision of adoption of state of the art, modern, digital, effective and efficient ways and means of doing business.

2. Purpose for RFP

The purpose of this Request for Proposal (RFP) is to invite bids from qualified and well reputed IT firms, legally registered in Pakistan and compliant with all applicable tax regulations, for the **Provisioning of Managed Services and 24/7 NOC Operations for CDNS's Data Centers**

Through this RFP, CDNS seeks to engage a competent service provider with proven expertise in delivering secure, scalable, and highly available data center solutions that meet the technical and operational requirements of hosting a critical financial business application. The selected firm will be responsible for the provisioning, installation, configuration, management, and ongoing support of the hardware infrastructure for the CBA of CDNS, ensuring its compliance with industry standards, security protocols, and regulatory requirements.

The scope of this RFP includes:

- The SERVICE PROVIDER should /manage compute, memory, storage, network and security devices and other fundamental computing resources including Operating system, Databases, Hypervisors and Infra etc. ORACLE Licensing and all hardware and accessories will be provided by CDNS.
- Implementation & support/troubleshoot/managed services should include provision of VMs, Bare metal physical servers as applicable, configuration of network, security devices and HW&CI, OS installation, DB setup, Hypervisor Installation etc.
- The Managed Services shall have deployment and operation support including, but not limited to, design, architecture, implementation trouble shooting and support of all the proposed/installed available HW& CI components including software, Patches, updates, configuration etc.
- Networks & communications must be managed by SERVICE PROVIDER such that, both PR & DR sites be synchronized and updated on real time basis and switching between both sites should be seamless and transparent to **field offices/ NSCs/Sites etc.**
- Administrative maintenance of data center, infrastructure and network devices provided by CDNS
- Ensuring high availability, data security, patching/updates, disaster recovery, and business continuity with the help of OEM.
- Providing 24/7*365 monitoring, incident management, and service desk support for the CBA's hosting environment. (it should be comprehensive, instead of CBA only).

CDNS aims to ensure that its core financial systems remain robust, secure, resilient, and capable of supporting its expanding digital financial portfolio in line with the Government of Pakistan's national financial digitization and inclusion agenda.

3. Background

The Central Directorate of National Savings (CDNS) operates its own Core Business Application (CBA of CDNS), which serves as the central platform for managing its wide range of savings, investment, and financial products. Over the years, CDNS has continued to enhance and expand the capabilities of its CBA in alignment with its national digitization strategy and the Government of Pakistan's broader financial inclusion objectives.

As part of this modernization journey, CDNS has successfully introduced several new modules and integrations into the CBA, including a comprehensive AML/CFT Transaction Monitoring System, the creation of Islamic Savings Products within the core platform, integration with the RAAST Micro Payment Gateway (MPG) of the State Bank of Pakistan (SBP), and the migration of legacy savings products from the Pakistan Post Office Department (PPOD). In addition, CDNS has launched digital savings accounts and digital securities providing customers with easier, faster, and more secure access to national savings products.

These initiatives have not only strengthened CDNS's operational efficiency and compliance readiness but have also positioned the organization as a key public-sector player in Pakistan's digital financial ecosystem.

Building on this momentum, CDNS now seeks to continue its digital transformation by engaging a qualified service provider for managed services necessary to run the CBA of CDNS. The objective is to ensure that the core application and its integrated modules remain secure, reliable, and scalable to support future functional enhancements, regulatory updates, and technological advancements while maintaining high levels of availability and data security.

CDNS currently operates its branch operations on a centralized application, the Core Business Application (CBA of CDNS), which was custom-designed, developed, and tailored using the state-of-the-art technologies. The CBA of CDNS was originally built to address the operational needs identified in 2017 and has since been continually enhanced with multiple modules and integrations, including a robust AML/CFT transaction monitoring system and integration with SBP's RAAST, Micro Payment Gateway (MPG). Presently, about 376 branches (NSCs) are utilizing the CBA of CDNS for their daily business operations.

4. High Level Scope of Work and Deliverables as mentioned in Annexure-A of RFP

The CBA of CDNS is accessed by NSC/branch staff, regional and central teams, and other CDNS personnel for various purposes. As financial legislation and digital service needs evolve, CDNS continues to face new requirements to ensure its platform remains compliant with industry best practices, secure from internal and external threats and vulnerabilities, and future-ready. To support this ongoing growth and evolution, CDNS now seeks to engage reputable **service provider** for the **Provisioning of Managed Services and 24/7 NOC Operations for CDNS's Data Centers**. This managed service must provide continuous availability, scalability, and security to meet the organization's current and future operational demands.

The scope of this RFP includes management of the existing HW&CI of CDNS, as well as the provisioning of ongoing managed services for future enhancements and integrations, as further elaborated in **Annexure-A** of this RFP.

5. Format for Technical Proposals & Evaluation Criteria

The technical proposal should be comprehensively prepared, structured and presented to include, but not necessarily be limited to, the following information. Support material should not be part of the main proposal but should be placed in annexures:

- Company profile
- Technical Proposal
- Support & Managed Services Structure
- Operational Structure of the organization

Note: During the technical evaluation, a bidder or all bidders may be called for technical presentation/clarification/demonstration of the proposed solution or equipment at their own cost (if desired by the CDNS).

5.1 Responsiveness Test/Initial Screening Criteria

Participating firm must meet all Responsiveness Test/Initial Screening Criteria, otherwise their bids will be rejected straight away.

S.no	Responsiveness Test/Initial Screening Criteria	Evidence required
1	Firm/JV must be 100% compliant of Scope of Work mentioned Annexure-A and terms and conditions of this RFP **(Mandatory)**	Submit compliance of Scope of Work on letter head with signed and stamp
2	Firm/JV must be registered company in Pakistan with SECP **(Mandatory)**	Provide Registration with SECP
3	Firm/JV must be registered with Taxation department and are on Active Tax Payer List with the registration status for Income Tax as "ACTIVE" and for sales Tax "OPERATIVE". **(Mandatory)**	Provide valid documentary evidence
4	Firm/JV must have atleast one office at Islamabad **(Mandatory)**	Provide documentary evidence
5	Firm/JV must have technical professional having relevant certifications in: a) **HPE (ASE),** b) **ORACLE (OCP) and** c) **Networks (NSE3 or JNCIP)** **(Mandatory)**	Provide copies of certifications issued by OEM/ Principal
6	Firm/JV must have at least one ongoing or completed project in which they are delivering or delivered managed or support services or SLA of Data Center Infrastructure, in last three years. **(Mandatory)**	Provide Documentary evidence
7	Firm/JV must have cumulative annual Turnover of minimum Rs.150 Million in last Three (3) Years. (Attach copies of the Audited Financial Statements). **(Mandatory)**	Bidder must share the audited financial statements of past three years.
8	Firm/JV should not have been blacklisted by any Government Department **(Mandatory)**	An undertaking duly attested by Notary Public/Oath Commissioner on a Stamp Paper that the bidder is not blacklisted by any Federal and Provincial Government department.
9	Bid security as an earnest money of required amount and shape shall be submitted to CDNS (in original) on technical bid opening date **(Mandatory)**	Provide Bid Security to CDNS (in original) on technical bid opening date.

5.2 Detailed Technical Evaluation Criteria (50 Marks)

Technical Evaluation Criteria (50 Marks)						Distribution of Technical Marks
5.2.1	**Financial Strength (Rs. In Million)** >= 200 Million =8 >= 190 Million = 7 >= 170 Million = 6 >= 150 Million = 5	Provide Financial document / statement describing annual business turnover of **last three (3) years.** (Submit related documents).	**Year** 2025 2024 2023	**Rupees** Rs._____ Rs._____ Rs._____ Total Rs._____	Place at Page No.___ of Bid Place at Page No.___ of Bid Place at Page No.___ of Bid	**08**
5.2.2	**Experience in years (a)** Experience for Provisioning of Managed or Support Services or SLA of Data Center Infrastructure. >= 8 years = 8 marks >= 7 years = 7 marks >= 6 years = 6 marks >= 5 years = 5 marks >= 4 years = 4 marks >= 3 years = 3 marks **(Number of Years)**	Provide proof for ongoing or completed projects in which they are delivering or delivered managed or support services or SLA of Data Center Infrastructure **(Number of Years)** (Submit copy of supply order or work order or contracts or agreements)	**Year**	**Supply order/ Work order/contracts/ agreements**	Place at Page No.___ of Bid	**08**
5.2.3	**Experience/ Client (b)** Experience for Provisioning of Managed or Support Services or SLA of Data Center Infrastructure in	Provide proof for ongoing or completed projects in which they are delivering or delivered managed or support services or SLA of Data Center Infrastructure in Government / Private Sector **(Number of Projects)**	**Qty/ Number**	**Supply order/ Work order/contracts/ agreements**	Place at Page No.___ of Bid	**08**

	Government / Private Sector 4 and above projects = 8 3 projects = 6 2 projects = 4 1 projects = 2 **(Number of Projects)** **Note: Each project cost shall not be less than Rs. 50 Million, i.e the cost of project less than 50 Million shall not be considered for marking.**	(Submit copy of supply order or work order or contracts or agreements)				
5.2.4	**Offices** 1 marks ISB and 1 mark for Lahore	The company/ firm have offices in Islamabad and Lahore (Submit document).	Office-1 Office-2	Address_____ Address_____	Place at Page No.___ of Bid Place at Page No.___ of Bid	**02**
5.2.5	**Technical Human Resource (a)** **(Number of technical professionals in field of HPE Infrastructure)** 2 mark for each required professional (HPE Infra)	The bidder/company/ firm have **total numbers of technical professionals at his disposal** having experience of atleast five years in the field of **HPE infrastructure** across the Pakistan. (Submit proof of experience.)	1.Proof of Experience_____		Place at Page No.___ of Bid	**08**

5.2.6	**Technical Human Resource (b)** **(Number of technical professionals in field of Networking)** 2 mark for each required professional (HW&CI)	The bidder/company/ firm have **total numbers of technical professionals at his disposal** having experience of atleast of five years in the field of Networking **i.e Core Firewalls (Juniper or Fortinet)** across the Pakistan. (Submit proof of experience.)	Proof of Experience_____	Place at Page No.___ of Bid	**08**
5.2.7	**Technical Human Resource (C)** **(Number of technical professionals in the field of Software)** 2 mark for each required professional (Software)	The bidder/company/ firm have **total numbers of technical professionals at his disposal** having experience of atleast of five years in the field of **ORACLE (RAC, Data Guard, Backup & Recovery), LINUX and VMWare (vSphere, HA, DRS, vSAN)** across the Pakistan. (Submit proof of experience.)	Proof of Experience_____	Place at Page No.___ of Bid	**08**
				Total Marks	**50**

5.3 Acceptance Criteria

The bidders are required to submit bids as per PPRA Rule 36 (b) Single Stage - Two Envelopes Procedure Therefore, the proposals will be evaluated technically first **whose bis(s) qualify the responsiveness test/initial screening criteria**. Technical & Financial bids shall carry 50 and 50 marks respectively. 30 out of 50 marks are the qualifying marks for Technical bids. Financial bids of only technically qualified bidders will be opened, the financial bids of disqualified bidders shall be returned unopened. The date of opening of financial bids for technically qualified venders will be communicated later on.

The marking weightage will be as follows.

Technical Proposal (T) = 50 Marks. (30 qualifying marks)

Financial Proposal (F) = 50 Marks.

Total (T+F) = 100 Marks.

The technical proposals/bids securing 30 i.e. 60% of total marks allocated for Technical Proposals or more in the technical evaluation will qualify for the next stage, i.e. financial opening. The bidder whose quoted prices are lowest will get the maximum marks (i.e. 50 marks) in financial evaluation using formulae given below:

(A) Bid ratio = (a) Lowest quoted price / (b) Quoted price for which financial marks are required [for lowest it would be 1]

(B) Bid ratio x 50 = Financial marks of (b)

The cumulative effect of both Technical and Financial marks shall determine position of the bidders. The contract may be awarded to the vendor/bidder whose bid is approved on the basis of evaluated to be **"Most Advantageous Bid"** as per PPRA Rules.

6. Format of Financial Proposal

6.1 Compliance

A statement to the effect that Firm/Bidder comply to all terms and conditions mentioned in this RFP be submitted in Technical and Financial Bid.

6.2 Financial

The financial proposal should be provided in following format (all costs must be mentioned in Pak-rupees otherwise bid would be rejected straightaway)

Financials for Provisioning of Managed Services and 24/7 NOC Operations for CDNS's Data Centers (PR &DR Sites)

S. No	Item	Rs. with all applicable taxes
1.	**1st Year Managed Services and 24/7 NOC Operations**	
2.	**2nd Year Managed Services and 24/7 NOC Operations**	
3.	**3rd Year Managed Services and 24/7 NOC Operations**	
4.	**4th Year Managed Services and 24/7 NOC Operations**	
	Total (Rs)	

7. Terms of Reference

7.1 General

a. Bids should be submitted very carefully according to instructions within due date and time, failing which the bid will be rejected.
b. The language of the bid is English
c. Bidders are advised to quote only one option for the required solution, otherwise bid shall not be considered for further processing and sealed Financial bid be returned un-opened.
d. Amendments in the bids must be signed and stamped.
e. Bidder must have physical location of business, telephone numbers and email address and must provide proof of their existence in the business.
f. Bids received will be evaluated technically as per evaluation criteria given in the bidding document.
g. The bids received after the due date and time will not be entertained.
h. The right to reject and cancel any bid/proposal (for which reason may be conveyed if desired) is reserved by procuring agency. The CDNS's decision will be final and binding in all matters relating to this RFP.
i. Incomplete bids in any respect may be rejected by procuring agency.
j. CDNS reserves the right to cancel this RFP and reject all bids at any stage of the bidding process.
k. All the pages of bid document must be signed and stamped by authorized person of the bidding firm
l. The tentative Payment Schedule will be as follow however final payment schedule shall be covered in signed agreement with successful bidder

Monthly managed services payments will be paid to the successful bidder monthly basis after services rendered.

7.2 Bid Security / Bid Bond

a) Bid Security is acceptable **in the shape of a Bank Draft/Pay Order/ CDR only** of Pak-rupees in favor of CDNS, Islamabad should be submitted along with the sealed **"Technical proposal"**, **without which the proposal shall not be entertained/ accepted**.
b) The amount of the financial bid and bid security shall be in Pak Rupees otherwise bid would be rejected straightaway.
c) If the bid is withdrawn before the expiry of its validity the bid security will be forfeited in favor of CDNS, Islamabad.
d) The bid security of successful bidder will be retained till the submission of bank guarantee (BG)/CDR and that of other bidders will be released after the signing of agreement /submission of BG/CDR whichever is earlier by the successful bidder at appropriate time.
e) The prices quoted shall correspond to 100% of the requirements specified. Changes or revisions in rates after the opening of the bids will not be entertained and lead to disqualification of bid besides forfeiture of bid security in favor of CDNS.
f) In case selected bidder is not willing to perform the job, then the Procuring Agency may consider second Most Advantageous bidder for award of contract and so on if deemed fit.

7.3 Validity of proposal

All proposal and price shall remain valid for a period of at least 180 days from the closing date of the submission of the proposal.

7.4 Currency

All currency in the proposal shall be quoted in Pak Rupees (PKR).

7.5 Contracting

The selected vendor will sign Contract agreement on Rs: 5,000/- stamp Paper within twenty (20) days of issuance of Work Order for which draft may be obtained from Procuring Agency.

7.6 Penalty

During the contract period executed between CDNS and the Service Provider, for delay in the implementation schedule given at Annexure-B as well as failure to comply with the provision of providing the required services during the execution period of the agreement. CDNS shall impose penalty @ 0.5% per hour of the contract price/value of one year. This may also lead to the blacklisting of the company if feels appropriate by the CDNS. However, CDNS may relax the penalty clause, if penalty imposed, upon satisfactory and convincing justification by the service provider depending upon the nature and sensitivity of the job/ activity.

7.7 Governing Law

This RFP and any contract executed pursuant to this tender shall be governed by and construed in accordance with the laws of Islamic Republic of Pakistan. The Government of Pakistan and all bidders responding to this RFP and parties to any contract executed pursuant to this RFP shall submit to the exclusive jurisdiction to Courts at Islamabad only.

8. Instruction to Bidders

8.1 Communication

Enquiries regarding the RFP should be submitted or communicated to following contact details

Name:
Contact:
Email:

8.2 Submission of Proposal

Bidder must submit their proposal electronically within due date and time

8.3 Mode of Delivery of Bids and Address

Proposals shall be delivered by electronically through PPRA EPADS system.

Late submission of the Proposals shall not be entertained

8.4 Bank Guarantee ("BG")/CDR

The successful bidder shall be required to submit CDR (Call Deposit Receipt) or an un-conditional and irrevocable ("BG") on stamp paper, a sum equivalent to 02% (two percent) of the contract value of three years and valid for three years from the date of signing of the agreement. The ("BG")/CDR may be released by the CDNS after successful completion of contract period. The ("BG")/CDR shall be submitted on or before raising invoices. This ("BG")/CDR shall be issued by any scheduled bank operating in Pakistan and will remain valid until the final and formal termination of Contract by CDNS. The CDNS may forfeit the ("BG")/CDR if the bidder`s performance found to be poor or bidder breaches any of its obligations under the contract agreement or published RFP besides considerations for black listing the selected supplier or any other action taken under the law or all or waive off all or partially based on sound justification that may be beyond suppliers normal control, provided by the supplier and up to the satisfaction of CDNS but the decision in this regard would be at sole discretion of the CDNS and in no way, the supplier may consider it as its Right.

8.5 Disclosure/ Integrity Pact

Bidder/Vendor hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan (GoP) or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing the Bidder/Vendor represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

By signing this agreement, the Bidder/Vendor certify that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

By signing this agreement, the Bidder/Vendor accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, Bidder/Vendor agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by Bidder/Vendor as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form GoP.

8.6 Force Majeure

A "Force Majeure Event" shall mean act of God or any event or circumstance or combination of events or circumstances that are beyond the control of a Party and that on or after the date of signing of this Agreement, materially and adversely affects the performance by that Party of its obligations or the enjoyment by that Party of its rights under or pursuant to this Agreement; provided, however, that any such event or circumstance or combination of events or circumstances shall not constitute a "Force Majeure Event" within the meaning of this Section to the extent that such material and adverse effect could have been prevented, overcome, or remedied in whole or in part by the affected Party through the exercise of due diligence and reasonable care, it being understood and agreed that reasonable care includes acts and activities to protect the Sites and the Facilities, as the case may be, from a casualty or other reasonably foreseeable event, which acts or activities are reasonable in light of the likelihood of such event, the probable effect of such event if it should occur and the likely efficacy of the protection measures. "Force Majeure Events" hereunder shall include each of the following events and circumstances that occur inside or directly involve Pakistan, but only to the extent that each satisfies the above requirements:

i. any act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act or campaign of terrorism, or sabotage;
ii. strikes, works to rule or go-slows that extend beyond the Sites, are widespread or nationwide;
iii. Change in Laws of Pakistan;
iv. Other events beyond the reasonable control of the affected Party, including, but not limited to, uncontrollable events, namely, lightning, earthquake, tsunami, flood, storm, cyclone, typhoon, or tornado, epidemic or plague, radioactive contamination or ionizing radiation;

8.7 Amicable Settlement/Dispute Resolution

Any dispute, controversy or claim arising out of or relating to this Contract, or the breach, termination or invalidity thereof, shall be resolved through negotiation in an amicable and friendly manner between the parties. The Parties shall seek to resolve any dispute amicably by mutual consultation and discussion at the appropriate level of Parties or through the committee constituted, representing members from both sides, whichever is suitable to reach the amicable solution of dispute.

If either Party objects to any action or inaction of the other Party, the objecting Party may file a written Notice of Dispute to the other Party providing in detail the basis of the dispute. The Party receiving the Notice of Dispute will consider it and respond in writing within thirty (30) days after receipt. If that Party fails to respond within thirty (30) days, or the dispute cannot be amicably settled within thirty (30) days following the response of that Party, Following shall apply.

Disputes shall be settled by arbitration in accordance with the following provisions:

1. Failing amicable settlement, the dispute, differences or claims, as the case may be, shall be finally settled by binding arbitration in accordance with the provisions of the Arbitration Act 1940 of Pakistan.
2. The arbitration shall be conducted at Islamabad, Pakistan before an arbitration panel comprising three (3) members, one to be nominated by each Party and the third nominated by the first two nominees (collectively, "arbitration panel").
3. The fees and expenses of the arbitrators and all other expenses of the arbitration shall initially be borne and paid equally by both the Parties, subject to determination by the arbitration panel. The arbitration panel may provide in the arbitral award for the reimbursement to the prevailing party of its costs and expenses in bringing or defending the arbitration claim, including legal fees and expenses incurred by such Party.
4. Any decision or award resulting from the arbitration shall be final and binding upon the Parties. The Parties agree that the arbitral award may be enforced against the Parties to the arbitration proceedings or their assets, wherever they may be found, and that a judgment upon the arbitral award may be entered in Honorable Courts having jurisdiction at Islamabad only.
5. Pending the submission of and/or decision on a dispute, difference or claim or until the arbitral award is published the Parties shall continue to perform all of their obligations under the Contract.

Annexure -A

Requirements/Scope of Work

CDNS is inviting bids from well reputable firms/ Technology / computer companies for the following requirements:

1. Project Objective

The objective of this engagement is to onboard a qualified Managed Services Provider (MSP) to assume operational responsibility for the Customer's existing IT infrastructure at the Primary (PR) and Disaster Recovery (DR) sites. The selected MSP will be responsible for 24/7*365 NOC Monitoring, Routine Operations, Incident Management, and the deployment of a customizable Network Management System (NMS) to ensure high availability and performance. The bidder shall establish in-house Network Operations Center (NOC) at its own premises specifically for CDNS. The service provider shall provide a view of NOC at CDNS premises. The service provider shall responsible to depute a Resident Engineer at CDNS, during the office hours.

2. Scope of Services

The MSP shall provide the following services:

2.1. NMS Deployment & Integration (In-Scope Deployment)

I. **Tool Deployment:** The MSP is responsible for provisioning, deploying, configuring, and their own Network Management System (NMS) / Monitoring at CDNS. The deployed solution must provide complete monitoring coverage for all equipment and systems listed in Annexure-A.

II. **Integration:** Integrate the NMS with the Customer's existing hardware and software assets (listed in Annexure-A) to enable real-time telemetry.

III. **Dashboard Extension:** Provide a "Single Pane of Glass (SPOG)" dashboard view to the Customer, offering visibility into infrastructure health, uptime, and performance metrics.

2.2. 24/7*365 NOC Monitoring Services

I. **Real-Time Monitoring:** Resource provisioning to ensure continuous 24/7*365 monitoring of all servers, storage systems, network devices, software, application and security appliances at both PR and DR sites.

II. **Alert Management**: Proactive identification and notification of threshold breaches, including CPU, memory, disk utilization, bandwidth usage, and latency issues.

III. **Event Correlation**: Intelligent filtering and correlation of security events to differentiate real incidents from routine alerts or false positives.

IV. **Periodic Reporting**: Delivery of regular reports covering overall performance, service availability, and operational status.

V. **Core Link Monitoring**: Continuous monitoring of core links, including bandwidth utilization and trend analysis.

VI. **IPsec Tunnels / VPN Management**: Creation, monitoring, and health tracking of IPsec tunnels and VPN connections Core and Branch level.

VII. **VLAN Management**: Configuration and management of VLANs as required.
VIII. **Trend and Insights Reporting**: Preparation of analytical reports providing performance trends and operational insights.
IX. **Kubernetes, Virtualization & OS Monitoring Coverage:** The deployed NMS shall deliver full-stack monitoring for Kubernetes clusters, virtual machines (VMs), containers, and operating systems, including resource utilization, pod health, node status, cluster performance, and service uptime.
X. Continuous 24x7x365 monitoring
XI. Event, incident, and alert management

2.3. Managed Services & Routine Operations

I. **VM Provisioning:** Creation, reconfiguration, and resource allocation of Virtual Machines (VMware vSphere) as per Customer requests.
II. **Health Checks:** Daily/Weekly routine health checks of all critical infrastructure components.
III. **Backup Management:** Monitoring of Veeam backup jobs; re-initiating failed jobs and ensuring data integrity.
IV. **Database Support:** Basic Level 1/Level 2 support for Oracle 19c (start/stop services, basic troubleshooting, monitoring tablespaces).
V. **Capacity Planning:** Monitoring resource utilization (CPU, RAM, Storage) and providing recommendations for future scaling.

2.4. Incident Management

I. **L1/L2 Support:** Diagnosis and remediation of operational issues.
II. **Vendor Escalation:** Acting as the technical liaison to escalate hardware failures (e.g., failed drives, PSU) to the respective OEMs (HPE, Cisco, Juniper, Fortinet) under the Customer's existing support contracts.
III. **Ticketing System:** Handle and track the full lifecycle of all incidents through the NOC ticketing system.
IV. **Root Cause Analysis (RCA):** Provide RCA reports for all Severity 1 incidents

2.5. Migration of Software/Applications/Configurations

The Service Provider will be responsible for migration and configuration of any software/applications/configurations from one Hardware to another Hardware installed at PR& DR Sites

2.6. Assets Monitoring

The Service Provider will be responsible for the monitoring and routine operation of the Hardware and Communication Infrastructure (servers, storage and network devices) installed or to be installed (in future) at PR and DR Sites of CDNS.

2.7 . Management of Database

The Service Provider is responsible for managing database platforms, including backup, restoration, optimization, and recovery operations. Setting up asynchronous data replication between the primary and secondary environments.

2.8 . Disaster Recovery Planning

The Service Provider shall conduct DR Drill Activity at least twice annually, Assistance in creating a policy with RPOs/RTOs for different services, 99.9% uptime commitment.

2.9 Detail requirements/Scope of Work

a) Maintenance and managed services for Infrastructure, System Administration and Operating Systems

1. Monitoring of Rancher environment
2. Maintenance of nodes / alerts check on Kubernetes cluster
3. Configuration & Management of alerts on transaction for higher than normal rejection as well as inactivity
4. Configuration & management of alerts on all application servers for monitoring of memory usage, CPU usage, storage utilization. (Open Source Tool)
5. Configuration & management of alerts for network monitoring at application level (for interfaces with internal and external entities).
6. Setting up of alerts/reporting server
7. Connecting vCentre
8. Provisioning of open source monitoring applications
9. Installation and configuration of Database
10. Installation and configuration of middleware (GitLab, Jasper, MailEnable, Nginx reverse proxy, JIRA, etc.)
11. Installation and configuration of monitoring tools (SolarWinds, Nagios, Grafana)
12. Kernel updates, security patches and hotfix deployment
13. OS cluster management including Kubernetes node OS layers
14. Snapshot management and lifecycle cleanup
15. Storage connectivity and zoning for virtual machines across SAN switches
16. Co-ordination with Hardware vendor on SLA's & routing firmware upgrades of hardware deployed on the CDNS customer site.
17. HPE Synergy 12000 chassis, Blade 480 Gen10 firmware/driver updates
18. Coordination for replacement, RMA and hardware fault resolution
19. Kubernetes upgrade management
20. Backup of repositories and cluster configuration
21. Installation, configuration, patching, and maintaining Operating System, middleware, databases, and application dependencies.
22. Configuration of Nginx reverse proxy with SSL
23. Secure deployment pipelines, version control, patch management and ensure that platform changes do not compromise security and data availability. Backup of GitLab repositories
24. Management of all hardware/virtual environment, operating system's licenses and other pre-requisite software's license.
25. Software Installation
26. Installation of Operating Systems
27. Virtualization of Servers but not limited to:
28. Setting up of virtual machines
29. Setting up of alerts/reporting server
30. Connecting vCentre with Rancher
31. Co-ordination with Hardware vendor on SLA's & routing firmware upgrades of hardware deployed on the CDNS customer site.

32. Support and setting up monitoring /archiving/reporting tool.
33. Configuration & management of alerts on all application servers for monitoring of memory usage, CPU usage, storage utilization.
34. Configuration & management of alerts for network monitoring at application level (for interfaces with internal and external entities).
35. Deployment, configuration, and lifecycle management of VMware vCenter and vSphere 6/8
36. Provisioning, decommissioning and template management of virtual machines
37. Configuration of HA, DRS, vMotion and clustering
38. Deployment and patching of ESXi hosts on HPE Synergy Blade Servers and DR compute nodes
39. Hardware health monitoring and performance tuning of compute nodes

b) Managed services related to Database Administration including:

1. Configuration of Database replication between racks/Primary and DR Sites
2. Database configuration changes, table compaction or reorganization upon CDNS request;
3. Database software patch maintenance, up to one (1) point release upgrade per twelve (12) month period, each upon Customer request and approval;
4. Definition and implementation of any database backup and/or restoration methodology;
5. Regular Database Backup (incremental and differential).
6. Database problem resolution and incident management, including exclusive control over database startup and shutdown operations, executed upon CDNS approval.
7. Management of database security access
8. Alerts & notification setup that detects non-responsiveness or exceeded thresholds of database as per the requirements of CDNS
9. Installation and configuration of Database
10. Set up and management of Database Environment including Oracle RAC and Oracle Data Guard.
11. The Service Provider is responsible for managing database platforms, including backup, restoration, optimization, and recovery operations.
12. Setting up asynchronous data replication between the primary and secondary environments.

c) Managed services and required documentation of network switches at the PR/DR Site

1. Management of ACL as per the requirement of CDNS
2. Creating all IPSEC-VPN/Policy with in firewall.
3. IP Addressing within Infrastructure.
4. Firewall Configuration
5. Designing Primary Network Diagram
6. Creating ACLs
7. Creating VLANs
8. Creating IPSec VPNs at PR-DR Sites
9. Alerts setup and proactive monitoring of firewall with provided monitoring and reporting tools

10. The Service Provider will be responsible for designing and maintaining Primary and secondary Network Diagram (LLD & HLD).
11. The Service Provider is responsible for designing, deploying, and managing network infrastructure (i.e. switches, routers, firewalls, VPN gateways etc).
12. The Service Provider is responsible for ensuring proper network configuration and segmentation, VLAN, between core systems, DMZ, user LANs, and internet-facing components.
13. The Service Provider is responsible for firewall configuration and management, including quarterly rule reviews, version control, change management, and implementation of advanced security features (IDS/IPS, URL filtering, anti-malware, SSL/TLS inspection) .
14. The Service Provider is responsible for implementing and managing branch connectivity via secure VPN (IPSec AES-256 or stronger) with MFA for administrative access.
15. The Service Provider is responsible for redundant network paths, failover mechanisms, and disaster recovery readiness.
16. The Service Provider is responsible for continuous monitoring, alerting, and reporting on network performance, network configuration, security events, and uptime.
17. The Service Provider is responsible for ensuring network configuration and segmentation, VLAN, between core systems, DMZ, user LANs, and internet-facing components.
18. Implementation of micro-segmentation policies

d) Managed services of ticketing system ensuring

1. Ensuring up-time of system
2. Ensuring troubleshooting of any problem with respect to this RFP

e) Managed Services and Operational Support

1. Bidder to take handover from CDNS for the current infrastructure.
2. Provide day to day support to customer/CDNS for Infrastructure deployed on the primary and DR sites.
3. Monitor the assets deployed on CDNS primary and DR sites to ensure its compliance in terms of patches / upgrades with help of OEM.
4. Service Level Commitments for PR Site, 99.9% uptime commitment
5. Provide support on issues of following nature:
6. Performance bottlenecks
7. Health check-up
8. Security issues
9. Maintenance and managed services for System Administration and Operating Systems.
10. The Service Provider is responsible for supporting incident response, including containment, evidence preservation, root cause analysis, and post-incident reporting

f) DR (Disaster Recovery):

3. Virtualization of DR servers, replication, and backup processes.
4. Conduct **DR drills at least twice annually**, including failover and failback validation.
5. Assist in defining **RPO/RTO policies** for all services.
6. Ensure DR site uptime of 99.9% and regular security monitoring.

g) Reports to be submitted by Service Provider to CDNS (Daily/Weekly/Monthly etc.)

i.Performance and availability reporting to be submitted by the bidder.

- **Uptime and availability:** Reports on the operational status of servers, networks, and storage systems.
- **Latency and throughput:** Metrics on network performance, connectivity, and data transfer speeds.
- **Fault and incident reports:** Summaries of system failures, their causes, and resolution times.

ii. Security and compliance reporting to be submitted by the bidder.

- **Security audits:** Documentation of security control effectiveness, including firewall configurations, intrusion detection, and vulnerability scans.
- **Compliance status:** Reports demonstrating adherence to industry regulations like GDPR, HIPAA, or PCI-DSS.
- **Access control reports:** Audits of user access and permissions to sensitive data and systems.

iii. Resource and capacity management reporting to be submitted by the bidder.

- **Resource utilization:** Detailed reports on the usage of CPU, memory, storage, and bandwidth to identify bottlenecks and optimization opportunities.
- **Capacity planning:** Analysis of current resource usage to forecast future needs and prevent under-provisioning or overspending.
- **Asset management:** Prior intimation of maintaining Inventories of hardware and software assets, including their end of warranty, end of life and expiration announcements.
- **Updated Configuration Records:** Keep the configuration files in record of CDNS management and intimate in case of change in configuration, also keep the record of change history.

iv. Operational Reporting to be submitted by the bidder.

- **Backup and disaster recovery:** Regular reports on the status and success rate of data backups and restore tests.
- **Failover Drills:** Conducting drills with DR site with prior intimation and approved plans.
- **Drill Reports:** submission of reports after each drill covering the risk, failures and successors.

v. Third party performance Reports to be submitted by the bidder.

- **Connectivity Reports:** Regular report of outage in the links to CDNS management as well as the services provider.
- **SLA & Warranties:** Keep CDNS management updated about the under maintenance equipment status reports in coordination with the concerning Hardware provider till the closure of the case.

h)Hardware and Communication Infrastructure and software installed at Data Center, Islamabad and DR Site Lahore to be run by Service Provider.

Site	Category	Sub-Category	Equipment / Software	Qty	Description / Details
PR Site - Islamabad (CBA)	Compute	Chassis	HPE Synergy 12000 Chassis	1	Configure-to-order Frame
			HPE Synergy Composers	2	In chassis
			HPE Virtual Connect SE 40Gb F8 Module for Synergy	2	In chassis
			Brocade 16Gb/24 Fiber Channel SAN Switch Module for HPE Synergy	2	In chassis
			2650W Performance Hot Plug Titanium Plus FIO Power Supply Kit	6	In chassis
		Blade Servers	HPE Blade 480 Gen10 (16-core)	8	Intel Xeon-Gold 6130 (2.1GHz/16-core/125W)
			HPE 32GB (1x32GB) Dual Rank Smart Memory Kit	8x8	Per server
			HPE 400GB SAS 12G SSD	2x8	Per server
			Smart Array P204i-c SR Gen10 12G SAS Modular Controller	8	With 96W Smart Storage Battery
			3820C 10/20Gb Converged Network Adapter	8	Per server
			3830C 16Gb Fibre Channel Host Bus Adapter	8	Per server
		Blade Servers	HPE Blade 480 Gen10 (24-core)	4	Intel Xeon-Gold 6252 (2.1GHz/24-core/150W)
			32GB (1x32GB) Dual Rank x4 DDR4-2933	8x8	Per server
			960GB SAS 12G Mixed Use SFF SC Value SAS Multi Vendor SSD	2x8	Per server
			Smart Array P204i-c SR Gen10 (4 Internal Lanes/1GB Cache) 12G SAS Modular Controller	8	With HPE 96W Smart Storage Lithium-ion Battery
			3830C 16Gb Fibre Channel Host Bus Adapter	8	Per server

			4820C 10/20/25Gb Converged Network Adapter	8	Per server
		Rack Servers	HP DL380 Gen9	4	
			32GB Registered DDR4 RAM	4x4	Per server
			Intel Xeon E5-2683v4 (16 Core) 2.1GHz	2x4	Dual processors per server
			1.2 TB SAS 12G 10K RPM (2.5 inch) hot-swappable Hard Drive	8x4	Per server
	Storage	SAN Storage	HP 3PAR 8440 Storage	1	4N+SW Storage Field Base
			1.2TB+SW 10K SFF HDD	80	
			400GB SAS MLC SFF (2.5in) Solid State Drive (SSD)	16	
			1.8TB SAS 10K SFF (2.5in) HDD	40	24+16
			HPE 3PAR StoreServ 8000 SFF(2.5in) Field Integrated SAS Drive Enclosure	8	6+2
			SN6010C 12-port 16Gb Fibre Channel Switch	2	
		DAS Storage	HP MSA 2040	1	
			10TB LFF 3.5" 7.2K SAS Drives	10	100TB RAW capacity
		Tape Library	HP MSL 2024	1	
			LTO-7 standard media	48	24 media slots
	SAN	SAN Switches	Cisco SAN Switch (Brocade)	2	48 Ports Each 16G/FC, 12 Ports Active
	Network	Switches	Juniper EX4300	2	Aggregation Switches
	Security	Core Firewall	Juniper QFX5100	2	48 x 1/10G Optical Ports (SFP/SFP+), 4 x 40Gb QSFP, 1.4 Tbps Switching
		Core Firewalls	FortiGate 1100E	2	Core Firewall
			Juniper SRX 1500	2	NGFW: 12x1GbE RJ45, 4x1GbE SFP, 4x10GbE SFP+, 1x1GbE Mgmt, 1x1GbE HA, 1.7Gbps throughput
		Firewall	Fortinet 1000C	1	Firewall

			Fortinet 201E	1	18x GE RJ45, 4x GE SFP slots, NP6Lite & CP9 hardware accelerated, 480 GB SSD
			Juniper SRX 320	1	SBP Firewall
	Software	Virtualization	VMware vSphere 6	6 sockets	
			VMware vSphere 8	4 sockets	
			VMware vCenter	1	
		Database	Oracle 19c	24	Database licenses
		OS	Oracle Linux	1	Operating system
		Backup	Veeam Backup	16	Backup software licenses
			Nagios Core	NIL	Services Monitoring
		Container/Orchestration	Kubernetes	NIL	Application Cluster software
			Rancher	Implied	For Kubernetes management
		Applications	Jasper	NIL	Reporting
			GitLab	NIL	Repository (application performance monitoring)
			Mail Enable	12 core	Email relay
			Nginx	–	Reverse Proxy
PR Site - Islamabad (ADC)	Compute	Chassis	HPE Synergy 12000 Chassis	1	Configure-to-order Frame
			HPE Synergy Composers	2	In chassis
			HPE Virtual Connect SE 40Gb F8 Module for Synergy	2	In chassis
			Brocade 16Gb/24 Fiber Channel SAN Switch Module for HPE Synergy	2	In chassis
			2650W Performance Hot Plug Titanium Plus FIO Power Supply Kit	6	In chassis
		Blade Servers	HPE Blade 480 Gen10 (24-core)	4	Intel Xeon-Gold 6252 (2.1GHz/24-core/150W)
			32GB (1x32GB) Dual Rank x4 DDR4-2933	8x8	Per server
			960GB SAS 12G Mixed Use SFF SC Value SAS Multi Vendor SSD	2x8	Per server

			Smart Array P204i-c SR Gen10 (4 Internal Lanes/1GB Cache) 12G SAS Modular Controller	8	With HPE 96W Smart Storage Lithium-ion Battery
			3830C 16Gb Fiber Channel Host Bus Adapter	8	Per server
			4820C 10/20/25Gb Converged Network Adapter	8	Per server
		Blade Servers	HPE Blade 480 Gen10	4	Intel Xeon-Gold 6130 (2.1GHz/16-core/125W)
			HPE 32GB (1x32GB) Dual Rank Smart Memory Kit	4x4	Per server
			HPE 400GB SAS 12G SSD	2x4	Per server
			Smart Array P204i-c SR Gen10 12G SAS Modular Controller	4	With 96W Smart Storage Battery
			3820C 10/20Gb Converged Network Adapter	4	Per server
			3830C 16Gb Fibre Channel Host Bus Adapter	4	Per server
	Security	HSM	HSM Thales 9000	2	Cryptographic keys
	Network	Switches	Juniper QFX5100	2	48 x 1/10G Optical Ports (SFP/SFP+), 4 x 40Gb QSFP, 1.4 Tbps Switching
	Security	Firewalls	Juniper SRX 1500	2	NGFW (same specs as CBA site)
	Software	Virtualization	VMware vSphere 6	4 sockets	
		Database	Oracle DB	8 core	Database
		Operating System	RedHat Linux	–	Operating System
DR Site - Lahore	Compute	Storage	Huwei	1	95 TB
		Blade Servers	Huawei CH242 v5	2	4x14 core per server
	Network	Switches	Juniper EX4300	2	Aggregation Switches
	Security	Firewalls	Juniper SRX 1500	2	Core Firewall
			Fortinet 201E	1	18x GE RJ45, 4x GE SFP slots, NP6Lite & CP9 hardware accelerated, 480 GB SSD
		Firewall	Juniper SRX 320	1	SBP Firewall

	Software	Virtualization	VMware vSphere 6	1 socket	
			VMware vSphere 8	4 sockets	
			VMware vCenter	1	
		Database	Oracle 19c	24	Database
			Oracle Linux	1	Operating system
		Backup	Veeam Backup	16	Backup software
			Nagios Core	NIL	Services Monitoring
		Container/Orchestration	Kubernetes	NIL	Application Cluster software
		Applications	Jasper	NIL	Reporting
			GitLab	NIL	Repository
			Mail Enable	12 core	Email relay
			SQL Server	–	For SolarWinds SAM
			Nginx	–	Reverse Proxy

Annexure-B

Minimum commitment for SLA (Service level agreement)

a)Minimal Terms for SLA (Service Level Agreement)

1. Signed agreement between Service Provider and CDNS will remain effective for THREE YEARs from the signing of this contract and will be renewable with mutual consent for further one year.
2. Notwithstanding the foregoing, upon written notice to the other, either party may terminate this agreement upon three months prior written notice for failure of the other party to comply with any of its terms and conditions.
3. This agreement shall be governed by the laws of Pakistan and constitutes the complete and exclusive statement of agreement superseding all oral or written communications and any prior agreement between the parties relating to its subject matter

b)Scope of Services for SLA

Support Services will be provided with an aim to deliver quality technical support. Bidder agrees to provide managed services infrastructure as per details mentioned in the Annexure-A,

c)Severity Levels

The following standard problem definitions will apply to the services provided under the terms of signed agreement

Severity Level	Status	Impact
Severity 1	Mission Critical	▪ Business / Service has stopped ▪ The product is not functioning
Severity 2	Urgent	▪ Business is impeded but can continue to operate ▪ A major product feature not functioning
Severity 3	Medium priority	▪ Business not affected, but there are noticeable problems ▪ Functionality loss has an easy workaround
Severity 4	Low Priority	▪ No service impacts ▪ Request for information

Bidder agrees to provide services delivery as follows. (Resolution time must be reduced)

Severity Level	Response Time	On-Site Support	Resolution Time
Severity 1	15 Minutes	≤ 1hrs (If required)	6 Hours
Severity 2	30 Minutes	≤ 2hrs (If required)	12 Hours

Severity 3	3 Hours	(If required)	3 days
Severity 4	24 Hours	(If required)	7 Days

RACI Matrix (Summary)

RACI = Responsible, Accountable, Consulted, Informed

Activity	CDNS	Service Provider	Notes
Infrastructure Operations	I	R/A	Daily ops, monitoring, patching
VM & Server Provisioning	I	R	Lifecycle management
Network Management	I	R	LAN/WAN, firewall config
Security Monitoring	I	R	Alerts, incident escalation
DR Drills	A	R	CDNS approves drill schedule
Change Requests	A	R	Vendor executes after approval
License Management	R	I	CDNS provides licenses
New Hardware Procurement	A	C	Vendor recommends hardware
Upgrade Planning	A	R	Capacity planning & recommendations
Application Support	R	I	Infrastructure only support

Legend: ***R = Responsible, A = Accountable, C = Consulted, I = Informed***

d)Support Service Channels

All Support Services Channels that are available have been mentioned below whereas On-Site Support (Datacenter Islamabad/Lahore) will be provided from Service Provider as mentioned under section "Severity Levels". Coverage parameters specific to the service(s) covered in signed agreement are as follows:

1. 24 x 7 On-Site/Remote Support for Severity 1 & Severity 2 issues
2. Remote Support for Severity 3 & Severity 4 issues will be provided in *Standard Working Hours (9:00 AM to 5:00 PM Monday to Friday, excluding Public Holidays)
    - Telephonic Support
    - Email Support
    - Remote Desktop Support

* Standard Working Hours: 9:00 AM to 5:00 PM Monday to Friday, excluding Public Holidays

Helpdesk Ticketing System (support ticket system) will be provided by Service Provider that will collect all customer support requests from above mentioned Support Service Channels and manages them in an adequate Helpdesk Ticketing System.