CENTRAL DIRECTORATE OF NATIONAL SAVINGS

Request for Proposal (RFP)
For

Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS

Prepared By
Operations Wing

4th June 2022

Central Directorate of National Savings
Head Office: 23-N, Savings House, G-6 Markaz, Melody Market, Islamabad
Tel: 051 9215741-43 Fax: +92-51-9215761-62

(SAY NO TO CORRUPTION)

TENDER NOTICE

1. Sealed tenders are invited from well reputed firm(s) registered with Taxation Authorities and having their own well-established offices and supervisory structure for Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS.

2. The detailed **Request for Proposal (RFP)** which would be 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. The bids along with supporting documents in sealed separate envelopes (one for technical bid & other for financial bid) must reach at office of the undersigned latest by **29-June-2022 up to 10:30 A.M.** The envelopes/bids should be addressed to the undersigned. Bids will be opened on the same day at **11:00 A.M** 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. There will be a Pre-Bid Meeting/Demonstration regarding "Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS", to take onboard all prospective bidders who wish respond to RFP against this tender to enable them for preparation their Technical bids and Financial aspect in a more better and well aware way to meet the objective/scope of Tender/RFP. The venue will be the same as mentioned in Para 3 above **10:00 AM to 11:30 AM on Tuesday 14-June-2022**. So, all the prospective bidders, in their own interest, are advised to attend the Pre-Bid Meeting/Demonstration.

5. The Procuring Agency reserves the right to reject any/all or a part of bids for which reasons may be conveyed if desired in writing. A Bid Security is required and acceptable in the shape of a Bank Draft/Pay Order/Demand Draft/ Banker's cheque/CDR/Cashier Cheque only, issued from any scheduled bank operating in Pakistan, of PKR 100,000/- (Rupees one hundred thousand only), **placed in Technical Bid,** in the favour of **CDNS, Islamabad**.

6. For any query related to this Tender Notice, please feel free to contact the undersigned.

DIRECTOR (OPERATIONS)
Central Directorate of National Savings
Head Office: 23-N, Savings House, G-6 Markaz, Melody Market, Islamabad
Tel: 051 9215741-43 Fax: +92-51-9215761-62

SECTION – I

1.1 INTRODUCTION AND DISCLAIMER

This Request for Proposal document ("RFP") has been prepared solely to enable Central Directorate of National Savings ("CDNS") in the selection of suitable Consultant firm through tender for Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS as per given scope.

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between CDNS and any successful Bidder as identified after completion of the selection process as detailed in this RFP document.

1.2 INORMATION PROVIDED

The RFP document contains statements derived from information that is believed to be true and reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with CDNS in relation to the provision of services. Neither CDNS nor any its employees' gives any representation or warranty (whether oral or written), express or implied as to the accuracy, updating or completeness of any writings, information or statement given or made in this RFP document. Neither CDNS nor any of its employees' has carried out or will carry out an independent audit or verification or investigation in relation to the contents of any part of the RFP document.

1.3 FOR RESPONDENT ONLY

The RFP document is intended solely for the information of the party to whom it is issued/obtained from PPRA Website or be downloaded from National Savings Website i.e; www.savings.gov.pk ("the Recipient" or "the Respondent" or "the Bidder") i.e. Private Firm/ limited Company, partnership firm.

1.4 CONFIDENTIALITY

This document is meant for the specific use by the Respondents interested to participate in the current tendering process. This document in its entirety is subject to Copyright laws. CDNS expects the Bidders or any person acting on behalf of the Bidders to strictly adhere to the instructions given in the document and maintain confidentiality of information. The Bidders will be held responsible for any misuse of the information contained in the document and liable to be prosecuted by CDNS in the event of such a circumstance is brought to the notice of CDNS. By downloading the document, the interested party is subject to confidentiality clauses. CDNS may update or revise the RFP document or any part

of it. The Recipient acknowledges that any such revised or amended document shall be received subject to the same confidentiality terms.

1.5 DISCLAIMER

CDNS and its employees disclaim all liability from any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities expenses or disbursements incurred therein or incidental thereto) or damage (whether foreseeable or not) ("Losses") suffered by any person acting on or refraining from acting because of any presumptions or information (whether oral or written and whether express or implied), including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the Losses arises in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of CDNS or any of its employees.

While the document has been prepared in good faith, no representation or warranty, express or implied, is or will be made, and no responsibility or liability will be accepted by CDNS or any of its employees, in relation to the accuracy or completeness of this document and any liability thereof expressly disclaimed. The RFP is not an offer by CDNS, but an invitation for bidder's responses. No contractual obligation on behalf of CDNS, whatsoever, shall arise from the offer process unless and until a formal contract is signed and executed by CDNS and the Bidder.

SECTION – II

2.1 INTRODUCTION TO CDNS

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".

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).

3. CDNS is a premier financial institution offering retail government securities and savings products (known as National Savings Schemes (NSS)), level playing field to small savers through diversified product mix. It is a key contributor towards financial inclusion with an investor base of around 7 Million and a portfolio of about PKR ~4 trillion, which is around 33% of total banking deposits. Its share in domestic debt of government is around 24%. 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 373 National Savings Centres (NSCs). Apart from offering NSS through National Savings Centres (NSCs), these are also being offered through agency arrangements with Pakistan Post and network of commercial scheduled banks operating in Pakistan. Thus, outreach of NSS is in every nook and corner of the country.

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 impudent initiatives for revamping of CDNS business application software from distributed to centralized architecture. This includes offering Alternate Delivery Channels (ADCs), Biometrics, Debit 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.

2.2 Bid Submission Timelines/Deadlines

- Bids submission deadline: **29-June-2022 up to 10:30 A.M**
- Opening of Technical Bids: **29-June-2022 up to 11:00 A.M**

SECTION – III

3.1 RFP OBJECTIVE

3.1.1 CDNS has computerized all its branches across Pakistan through a centralized system having co-located Data Centre at NTC Islamabad and its DR site at NTC Lahore respectively. CDNS intends to develop and update a comprehensive Information System & Cyber Security Framework in compliance with ISO27001, and Data Management Framework and to provide services to fulfill the compliance and readiness for information security certification in line with ISO27001.

3.1.2 This will include but not limited to development of ISMS Scope, Asset base Risk Assessment, Risk Treatment plan, Internal and External Penetration Testing including Vulnerability Assessment along with information security policies, processes, SOPs and other relevant operational and technical documents on, but not limited to:

1. Data Loss Prevention (DLP), Data Encryption, Classification, Data Sharing
2. Access Control Policies, Privilege access management
3. Employee Management (on/off Boarding)
4. Asset Management
5. Cryptographic functions and its policies
6. Operations / Operational Security policies
7. Communication policies and security
8. All other related polices, processes, SOPs and all other relevant operational and technical documents relevant to information security required for information security compliance and readiness for certification
9. Patch management and remediation

with recommended remedial measures/actions/impacts on Periodical basis. Furthermore, the objective is to comply all major industry security standards [but not limited to] stated above.

3.1.3 To attain certification at appropriate time (if required) for its country wide operations including Data Centre and DR Site or any other IT facility of CDNS.

3.1.4 The scope will also include the managed services from the consultant/bidder in the shape of at-least 4 resident engineers to be deployed at CDNS office. The tentative JD/KPI/resources skills of these resident engineers are placed at Annex-A. In case there is any amendment/upgradation inside the frameworks/Standards the successful bidder will have to update the policies/Procedures and documentation accordingly for CDNS. Similarly, the Certifications will have to be upgraded accordingly for all or some of the

above-mentioned standards. For this CDNS intends to hire competent and qualified consultant through Managed Services Model.

3.1.5 The selected Bidder shall be required to independently arrive at approach and methodology, based on the above-mentioned standards, best practices, and guidelines, suitable for the CDNS, after taking into consideration the effort estimate for completion of the same, the resource and the equipment requirements.

3.1.6 CDNS expressly stipulates that the Consultant's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire assignment and that delivery of the deliverables and the services in connection therewith are only a part of the assignment.

3.1.7 The selected Bidder shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment at no additional cost to CDNS.

3.1.8 The selected Bidder will be responsible not only to develop, update the Procedures, Guidelines, IT Polices, Technical Documents, Governance and Security Related documents, ISMS Scope but also shall develop, update & reengineer a comprehensive Information System & Cyber Security Framework in compliance with the above-mentioned (or any other relevant) standards.

3.1.9 One of the key objectives of the RFP is to develop a CDNS network and security operations and related controls, therefore the successful bidder will have to develop the same for CDNS, manage the same through Managed Services and provide training, processes, and leadership to the CDNS resources for NOC & SOC operations

3.1.10 CDNS intends to set up a state-of-the-art NOC and SOC facilities including NOC Tools, to achieve this a Successful Bidder shall establish same under managed services by using a Unified Network Monitoring System, SIEM (Security Identity and Event Management) and SOAR (Security Operations and Automated Response) tools.

3.1.11 The successful bidder may be required to identify and provide software / tools and / or solutions that may be needed in accomplishment of Scope of Work and purpose of this RFP.

3.1.12 The Procuring agency reserve the rights to procure any or all services, software's either from the selected bidder or procuring agency may provide the same that may be needed in accomplishment of Scope of Work and purpose of this RFP.

3.2 SCOPE OF WORK

3.2.1 The scope of this RFP is to develop comprehensive Information System & Cyber Security Framework in compliance with ISO27001, and Data Management Framework and to provide services to fulfill the compliance and readiness for these certifications. This will include but not limited to development of ISMS Scope, Asset base Risk Assessment, Risk Impact Assessment, Risk Mitigation & Treatment plan, Internal and External Penetration Testing including Vulnerability Assessment, sensitivity level, Remedial measures, without harmful/disaster activity for the CDNS over all IT Setup/System, along with policies on but not limited to:

1. Data Loss Prevention (DLP), Data Encryption, Classification, Data Sharing
2. Access Control Policies, Privilege access management
3. Employee Management (on/off Boarding)
4. Asset Management
5. Cryptographic functions and its policies
6. Operations / Operational Security policies
7. Communication policies and security
8. All other related polices, processes, SOPs and all other relevant operational and technical documents required for information security compliance and readiness for certification
9. Patch management and remediation

With recommended remedial measures/actions/impacts on Periodical basis through Managed Services Model that would compromise of all CDNS Information assets at its PR & DR Site located at NTC Data Center at Islamabad and Lahore respectively, any other IT facility including all its field offices across Pakistan.

3.2.2 The information assets may largely be categorized into networks & communications, infrastructure, hosts/servers, hypervisor/VMs, endpoints (workstations), databases, applications, tools, utilities, APIs & Web Services, business critical information and critical business flow (either manual or automated) etc.

3.2.3 To assess the relevant risks, the Successful Bidder may conduct vulnerability assessment using automated vulnerability scanners to identify potential risks in information systems. The vendor will conduct IT Need Assessment in Compliance of the repeatedly mentioned ISOs & Cyber Security Framework

Development, and Data Management Framework along with other above mentioned standards.

3.2.4 Successful Bidder/Consultant will identify, assign criticality, and evaluate all information assets (data, information systems, IT and other processes, and information processing facilities) which store, maintain, support, or transmit business critical data, based on CIA triad. On the basis of Need Assessment carried out by the Successful Bidder and its recommendations thereof, CDNS may amend the scope of the work to meet the overall objective of effective Risk Assessment, Risk Mitigation, ISO Compliance and Certification.

3.2.5 Risk Assessment and treatment plan should be done as per above mentioned best practices and Standards of information security, Guidelines & framework for ISO27001 compliance.

3.2.6 The Successful Bidder would also develop or modify the risk assessment template with a scoring system which would be used by CDNS in consultation with the Successful bidder to assess risks at the in-scope centres and other units of CDNS.

3.2.7 Successful Bidder shall evaluate and measure the potential risk to the identified information assets (to include the cost of failure related to privacy and security breaches and any other information security threats (internal and external), Data breaches, Business interruption and network/communication damage, manual processes data leakages etc.) associated with how the different departments/divisions/wings/entities collect, use, manage, store, maintain, disclose, and dispose information. Assess whatever existing security measures are in place and the effectiveness of those measures. Furthermore, development, creation, improvements, implementation and maintenance of the information system and cyber security policies and procedure will be the responsibility of the Successful Bidder/Consultant.

3.2.8 Before/During the periodical assessment(s), the consultant should consider/ensure that the policies, standards, guidelines, procedures, practices (to be developed, implemented, and maintained/manage by the Successful Bidder/ Consultant), contractual requirements, other documents, and controls are in place and in line with the agreed comprehensive Information System & Cyber Security Framework and data center & data management framework that comply with listed above standards.

Scope of Work can be divided into activities / phases like

i. Activity/Phase 1
   a. –Information Technology and Information security Governance
      i. IT Need Assessment

ii. IT Governance Assessment
iii. BCP and DR Assessment
iv. Vendor Assessment
v. IT HR Assessment

b. Risk Assessment in guidelines with ISO27001 and assessment should well cover the
   i. Risk Impact
   ii. Risk Loss
   iii. Risk Action
   iv. Risk Requirement
   v. Risk mitigation
   vi. Risk Remediation
c. Establish, Evaluate and Structure the Risk Governance which includes
   i. CDNS Management Risk Governance
   ii. Role of CDNS Directors
   iii. Risk Management committee and its mandate
   iv. Information technology steering committee and its mandate
   v. Information Technology working committee and its mandate
d. Prepare Risk Treatment plan
e. Prepare ISM Scope document
f. Prepare policies processes and SOPs etc. in guidelines with ISO27001 for compliance and certification readiness
g. Detail assessment of Cyber security gaps and report along with strategic initiatives and procurement (if required). The report should have clear visibility of Cyber Security threats and its governance framework
h. Secure coding Platform and services of Core banking Application
   i. A modular, cloud-based/on premises solution for application security,
   ii. Dynamic Analysis (DAST), Interactive Analysis (IAST), Static Analysis (SAST), Software Composition Analysis (SCA), and Penetration testing
   iii. The solution Static Analysis (SAST) should help CDNS / partner developers quickly and accurately find and fix security flaws in proprietary code with detailed remediation guidance during each stage of software development

ii. Activity/Phase 2
   a. Managed Services for (Management, Implementations, configuration, and Security Operations)
      i. Implementation of people, process, and technology as per developed and approved policies, processes, SOPs and security framework during Phase-I
      ii. Guidance in procurement of additional technologies required
      iii. Provision and Management of Information and Cyber security operations (SOC) as a managed service
         1. Software/tools/licenses and solution for SOC
            a. SIEM tool need to be create the visibility of technology assets, traffic patterns, malicious activities, and guide

CDNS towards the right investments while deploying security solutions

b. Should support log aggregation, correlation, analysis, search engine and analytic capabilities
c. Should be able to highlight anomalies in CDNS IT environment
d. Should be able to ingest all type of data input forms CDNS IT infrastructure
e. Should be provide a granular interface
f. Should provide unlimited XDR capabilities
g. SOAR should have an integrated Incident Management, Cyber Threat Intelligence, Vulnerability Management, and Asset Management modules and risk scoring engine
h. The SOAR should provide enterprise class workflows and playbooks to support CDNS Operations and response mechanism to counter threats
i. The SOAR should integrate out-of-box with known cybersecurity products. All new integrations should be part of the proposal without additional cost
j. SIEM and SOAR solution must provide interoperable, compatible, vendor agnostic and scalable solution to meet seamless integration, interoperability, manageability and infrastructure/resource scalability requirements

iii. Activity/Phase 3
   a. Provision and Management of NOC operations as a managed service.
      i. NOC Software / Tool / Solution
         1. The NOC Software/Tool/Solution should be able to provide real time information to CDNS regarding the availability and performance of CDNS infrastructure which includes:
            a. Network, OS
            b. Servers and VMs
            c. Application, Databases, webpages, and Access management
   b. The NOC Software/Tool/Solution should be able to generate alerts and alarms once a performance threshold is breached
   c. The NOC Software/Tool/Solution should provide an integrated trouble ticket system for the NOC team to manage the faults
   d. The NOC Software/Tool/Solution should be able to generate reports on demand or scheduled. It shall be bidder responsibility to create report templates as per CDNS requirements and best practices.

iv. Activity/Phase 4
   a. Bidder must perform a VAPT activity minimum in n every quarter and to publish report to CDNS senior management.
   b. CDNS May request bidder to perform the VAPT on need basis as well

v. Activity/Phase 5
   a. CDNS User awareness workshops on:
      i. Information Security

ii. Cyber Security
iii. Data and Privacy
iv. Implementation of information and Cyber Security policies and processes
v. Technical Level-1 training on information and cyber security operation and management
vi. Technical Level-1 training on NOC operation and management

vi. Activity/Phase6
   a. Resident Engineer on site
      i. Bidder to provide two resources for Information security
      ii. Bidder to provide one resource for System
      iii. Bidder to provide one resource for infrastructure
      iv. CDNS may request more than one information security specialist on need basis.

ACTIVITY WISE DETAILED SCOPE OF WORK

The above Activities/Phases are further discussed in detail as below:

Activity/Phase 1 will cover complete information technology and information security governance and its assessment of Central Directorate of National Savings (CDNS) and all its offices / branches with a focus on relevant areas as follows:

1. Bidder should perform and evaluate the current IT Need Assessment and submit the current assessment report covering the areas but not limited to:
    i. IT Infrastructure and enterprise architecture assessment
    ii. IT Security Assessment
    iii. IT governance assessment
    iv. BCP and DR assessment
    v. Vendor Assessment
    vi. IT HR Assessment
2. Based on the assessment report Bidder should conduct a detailed asset-based risk assessment of complete technological and digital stack of CDNS.
3. Bidder should submit the detail risk assessment report with clear brief on impact, loss, action, requirements to mitigate and remediations. The successful bidder shall facilitate the CDNS to maximum extent for implementing the remediation measures.
4. Establish, evaluate and ensure the risk governance structures including the role of the directors/ risk management committee, working committee or steering committee, whichever is necessary, in defining risk management strategies (e.g. establishing and monitoring of risk limits).
5. Perform Risk Assessment and assess the level of independence and adequacy of the risk management function including staffing levels and reporting structure.
6. Review the Information System & Cyber security policies / framework (if already available with Central Directorate of National Savings (CDNS) otherwise develop the same) and recommend any improvements for future to fulfill the compliance and readiness for ISO27001 Certification followed by facilitation in certification (if needed by CDNS).
7. Assess MIS capabilities (current/in future) to generate timely and accurate information
8. Survey the Data center sites and analyze the non-compliance if any
9. Suggest and make final recommendations on how risk management can be improved through use of automated assessment and monitoring tools.
10. Review risk management reports (including Penetration practices and reports)and suggest how they could be strengthened (for instance, by improving internal analytical capacity and data quality/ Security etc.).
11. Business continuity planning, sustainability, and plan for secure and early disaster recovery.
12. Secure coding Platform and services of Core banking Application
    i. A modular, cloud-based/on premises solution for application security
    ii. Dynamic Analysis (DAST), Interactive Analysis (IAST), Static Analysis (SAST), Software Composition Analysis (SCA), and Penetration testing
    iii. The solution Static Analysis (SAST) should help CDNS / partner developers quickly and accurately find and fix security flaws in proprietary code with detailed remediation guidance during each stage of software development

Activity/Phase – 2 will cover the SOC implementation, configuration, and operations on managed services basis

1. By this stage the consultant will have the required information to select, deploy integrate a SIEM (Security Information and Event Management) system along with SOAR and GRC Compliance tool.
2. The purpose of the SIEM tool will be to create the visibility of assets, traffic patterns, malicious activities and will guide to CDNS towards the right investments while deploying security solutions.
3. The proposed SIEM tool should support log aggregation, correlation, analysis, search engine and analytic capabilities.
4. The SIEM should be able to highlight anomalies in CDNS IT environment.
5. The SIEM should be able to ingest all type of data input forms CDNS IT infrastructure.
6. The SIEM should be provide a granular interface.
7. The SIEM should have an integrated Cyberthreat Intelligence engine.
8. The SOAR should provide enterprise class workflows to support CDNS Operations and response mechanism to counter threats.
9. GRC tool should provide real time compliance with the relevant industry standards like, ISO 27001 etc.
10. The proposed SIEM solution must provide interoperable, compatible, vendor agnostic and scalable solution to meet seamless integration, interoperability, manageability and infrastructure/resource scalability requirements.

The bidder is advised to do a careful analysis of the CDNS existing systems, applications and networks and future expansion requirements for the next 3 years for sizing and dimensioning of the tools

Activity/Phase – 3 will cover the NOC implementation, configuration, and operations on managed services basis.

1. Bidder should provide NOC tools to establish CDNS NOC CDNS intends to establish their NOC based upon unified monitoring of its technology stack.
2. The monitoring system should be able to provide real time information about the availability and performance of CDNS IT infrastructure including network, security, OS, severs, VM's Applications, databases, Webpages and all data center equipment including power, cooling, fire suppression and access management system.
3. The monitoring tool should be able to generate alerts and alarms once a performance threshold is breached. The NOC should provide an integrated trouble ticket system in order for the CDNS NOC team to manage the faults.
4. The NOC tool should be able to generate reports on demand or scheduled. It shall be bidder responsibility to create report templates as per CDNS requirements and best practices.
5. It is expected from the bidder to perform a careful analysis of the existing CDNS IT infrastructure and propose the NOC tools with adequate licenses to manage the future expected growth of ~20% YoY

Activity/Phase – 4 will cover the periodic vulnerability assessment and Penetration.

1) Based on critical Risk Assessment which is submitted by the bidder during the Risk Assessment, the bidder will be required to conduct Bi-Annually (after every 6 months) Vulnerability assessments both Internal and External.

2) Annual Penetration Testing of both Internal and External CDNS Environment will be the responsibility of the vendor.

Activity/Phase – 5 User awareness and training workshops for CDNS users

1. Conduct detailed workshops with CDNS technology and operation users on submitted Risk assessment report to brief the impact and Mitigation Plan
2. Develop SOPs, Policies, Process in compliance with ISO 27001 which are highlighted during the Risk Assessment
3. Bidder should conduct a study on CDNS data and submit a detail data governance and management strategy but not limited to:
    i. Mobile device policy
    ii. Access control policy
    iii. Anti-malware policy
    iv. Backup policy
    v. Logging and management policy
    vi. Physical security policy
    vii. Software policy
    viii. Records retention and protection policy
4. Above submitted data management and governance strategy shall describe about the management practices and implementation priorities to mature the CDNS data governance and objectives but not limited to:
    i. Define and communicate the organization's data management strategy and roles and responsibilities
    ii. Establish the processes and infrastructure for metadata management
    iii. Define a data quality & data hygiene strategy
    iv. Establish data profiling methodologies, processes and tools
    v. Ensure a data quality assessment approach
    vi. Define the data cleansing approach
    vii. Manage the life cycle of data assets
    viii. Developdata archiving, retention and purging Methodology including facilitation in implementing the same
    ix. Manage data backup and restore arrangements
5. Assist CDNS to implement all the policies and process to comply all the controls related to ISO 27001 standards and Data Management
6. Bidder should Identify the Internal controls during the Risk Assessment and recommend the Automation Process.
7. Periodical Review of Risk Assessment, suggest and give recommendations to improve/ strengthen the internal controls by using automated assessment and monitoring tools.

Activity/Phase Phase 6: Managed Services

- The duration of the consultant/successful bidder engagement with CDNS will be for 3 years, extendable to further 2 years on already approved rates.
- The consultant will have to provide at-least 4 resident engineers inside CDNS environment for maintenance, upkeep, monitoring of the processes, controls adaptability and Testing etc. The resources will be dedicatedly placed inside CDNS office/environment. The quantity of the

resident engineers required can be increased as per the requirement of CDNS however the criteria for the resident engineer have to be met by the successful bidder.

- The consultant/successful bidder will have to devise a training program in Islamabad for the relevant CDNS departments relating to entire Technology Stack of CDNS. The level including contents of the training will be decided in coordination with CDNS during the currency of the agreement. Each year there may be multiple training sessions.
- Design and Supervise an Onsite team of CDNS resources (if available) for Onsite 24 x 7 operations of CDNS NOC including Red (defense) and Green (offensive team, creating attack scenario's) to meet the CDNS Security objectives. However it will be the sole responsibility of Successful Bidder to manage the NOC operations for the engagement period.
- The consultant will provide, team & function management and report to CDNS on weekly/monthly/periodical/need basis (as the case may be).
- Domain expertise (Systems, Networks, and Applications etc.) shall be the responsibility of the consultant and the bidder should size the team accordingly.
- Any other tool including but not limited to SOAR, GRC, Reporting, Incident Management and other security tools which may be required during the currency of agreement shall be the consultant/successful bidder responsibility.
- Further, it will be the responsibility of Successful Bidder to manage and implement SOC of entire technology stack of CDNS under managed services for the complete currency of the agreement, besides training and capacity building of in-house CDNS resources.

3.3 Exclusions

- During assessment if there are any solutions or products requirement. **The consultant will guide CDNS for the appropriate solution or provide that solution to CDNS if possible. The financial impact of such unforeseen requirements may be covered through addendum to agreement between CDNS and the successful bidder.**

- The resident engineers if required to travel to other CDNS locations/branch locations other than Islamabad. The travelling cost will be borne by CDNS.
- Technical Implementation will be the responsibility of CDNS teams and/or its vendors on board; however, the bidder will assist/support CDNS teams and/or its vendors on board according to the need of requirement / expertise.

3.4 EXPECTED DELIVERABLES

In addition to provision of required services/tasks/assignments under managed services model, as explained in this RFP, the selected vendor would provide the following documents (but not limited to):

a) High Level Project Plan with detailed Project Methodology for the phase-wise approach.
b) Current Assessment Report of Complete Technology Stack with strategic initiatives.
c) Information System and Cyber Security framework Gap Assessment Report as per ISO 27001, and Data Management Framework standard with summary and recommendations
d) Detailed risk assessment which includes description, impacts, risk treatment, Risk Mitigation Plan and remediation etc.
e) A prioritized list of realistic options/controls for enhancing security. The vendor may suggest different types of remediation options/controls (e.g. policy, procedure, technology or technical control) for each identified risk/vulnerable area.

f) Preparation of Documentation/Policies and procedures as identified in the Information System and Cyber Security Framework gap report e.g.
   - Information Security Management System (ISMS) Manual along with Scope.
   - Information Security Department (ISD) Organogram and ISMS organization structure.
   - Report on local and International 'Information Security/Cyber Security and Privacy' related Laws & Regulations that CDNS required to compliance with.
   - Revised ISMS Scope document (Scope for implementation and Scope for ISO compliance);
   - Develop revised ISMS documents including:
     - Information security policies
     - ISMS procedures, standards and guidelines

g) ISO 27001 Stage 2 Report compliance and Certification (if needed)

h) Dedicated Managed Services support for 3 years and at least 2 dedicated resources

f) Implementation of related hardware and software (if needed) to attain highest level of all related aspects of security.

g) Vulnerability assessment including Internal and External Penetration Testing reports as per provided/suitable frequency

h) ISO 27001 Gap Assessment Report and Compliance

i) quarterly training/workshop sessions each year at CDNS's Islamabad premises on IT Risk Assessment and awareness about latest ISO27001 /Data Management Framework/Penetration Testing/ Social Engineering along with training manuals/presentations

j) Information System and Cyber Security Framework readiness and Completion.

k) NOC and SOC operational manual

l) AS IS Diagram/status report of existing security and IT infrastructure

m) Information System Policy Document

n) Information System Security Policy Document

o) Data Security Policy Document

p) Communication and networks security document

q) Database Management Policy document

r) Database backup, preservation, archiving, restoration, purging etc. Policy document.

s) Performance tuning, health, hygiene policy document

t) User Management Policy Document

u) Login/ password credentials protection and change policy

v) Hardware dispose of Policy

w) Other related technical policy Documents that are relevant to Technology driven financial organization like CDNS.

SECTION – IV

4. OTHER TERMS

4.1. FIRM'S UNDERSTANDING OF THE RFP

In responding to this RFP, the firm accepts full responsibility to understand the RFP in its entirety, and in detail, including making any inquiries as necessary to gain such understanding.

4.2. GOOD FAITH STATEMENT

All information provided by in good faith CDNS through this RFP. CDNS makes no certification that any item is without error. CDNS is not responsible or liable for any use of the information or for any claims asserted there from.

Note: The absence of addressing any requirement of RFP in the Technical Proposal may result in the Technical Proposal being declared as "Non-Responsive" or "Poor Grading" which may lead to the disqualification of the Bidder.

4.3. TERM OF CONTRACT

The Contract for "**Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS"** will be 3 years from the effective date of the Contract, extendable to further 2 years on already approved rates.

4.4. PAYMENT TERMS

4.4.1. For services rendered pursuant to this RFP, the Procuring Agency shall pay The Selected Vendor as follows:

a. Invoices shall be cleared upon receiving the invoice along with necessary documentation/activity/deliverables. Incomplete claims shall be returned to vendor.
b. Payment processing time may be 30 days after receiving of Invoice and necessary documentation.
c. All payments shall be made through cross cheque in Pak Rupees.
d. Taxes shall be deducted at source as per government rules at the time of payment.
e. A certificate by The Selected Vendor to the effect that he had not claimed the relevant payment in his previous claims that have already been paid.
f. The Procuring Agency reserves the right to scale down the amount of invoice as per its satisfaction.

Payment Schedule (1st Year)

Year – 1 [S# 1 – 7]	Payment Plan (%age of yearly contract value)
Kick-off meeting and project plan	10%
Gap Assessment Report	15%
Risk Assessment Report	10%
Quarterly VAPT Report	10% (2.5% after each quarter)
Risk Assessment treatment	5%
Submission of ISMS Document for ISO27001	15%
Submission of Information and Cyber security policies, processes, guidelines, and SOPs	20%
Secure coding Platform and services of Core banking Application	15%

Payment Schedule (2nd Year)

Year – 2 [S # 1 -7, 8]	Payment Plan (%age of yearly contract value)
Quarterly Resident Engineer Performance Report	Quarterly Payment Against the Cost / Value Quoted for S # 8
Quarterly Implementation status report with revised Risk assessment impact and compliance readiness score	8% (2% after each quarter)
Quarterly VAPT Report	10% (2.5% after each quarter)
Implementation and managed services of NOC	40%
Implementation and managed services of SOC	32%
Quarterly Security User Awareness Session	10% (2.5% after each quarter)

Payment Schedule (3rd Year)

Year – 3 [S # 1-7, S # 8]	Payment Plan (%age of yearly contract value)
Quarterly Resident Engineer Performance Report	Quarterly Payment Against the Cost / Value Quoted for S # 8
Quarterly Implementation status report with revised Risk assessment impact and compliance readiness score	10% (2.5% after each quarter)
Quarterly VAPT Report	10% (2.5% after each quarter)
Managed services of NOC	25%
Managed services of SOC	25%
Quarterly Security User Awareness Session	10% (2.5% after each quarter)
Revised Gaps Assessment Report	10%
Final Report	10%

g. The above Payment Terms are tentative, and Procuring Agency shall finalize the Payment Terms or Payment Schedule with the Successful Bidder at the time of draft agreement preparation

4.5. INSTRUCTIONS FOR BIDDERS

4.5.1. Communication and Pre-Bid Meeting/Demonstration

A Bidder requiring any clarification of the RFP document shall contact the Procuring Agency in writing at the Procuring Agency's address specified in this clause. The procuring Agency will respond to any request for clarification, provided that such request is received three days prior to deadline of pre-bid meeting date as specified in the Tender Notice. The Procuring Agency shall forward copies of its response to all the Bidders who had attended the Pre-Bid Meeting, including description of the inquiry but without identifying its source. No queries/enquires received after three days prior to the Pre-Bid Meeting shall be entertained / responded by the Procuring Agency.

Enquiries/Clarification regarding this RFP shall be submitted in writing via email, prior to the three days prior to the Pre-Bid meeting (after which no query shall be responded) to:

Director (Operations)

Central Directorate of National Savings (CDNS),

Ministry Of Finance.

GOVERNMENT OF PAKISTAN

23-N, Savings House, G-6 Civic Center, Islamabad.

Direct: 051-921-5753, Fax: +92-51-9215761-62
Email: directoroperations@savings.gov.pk

4.5.2. Submission of Proposal

Separate technical and financial bids must be marked on envelops "**Procurement of Consultancy and Managed Services for IT Need Assessment in Compliance of ISO 27001 & Cyber Security Framework Development, and Data Management Framework for CDNS"** sealed and packed in another single envelope be submitted within due date and time. **The Bid Security must be attached in the Technical Proposals without which the proposal shall not be considered by the Procuring Agency.**

4.5.3. Mode of Delivery of Bids and Address

Proposals shall be delivered by hand or by Dak (through Pakistan Postal Service)/courier so as to reach the address given at clause 4.5.1 by the due date and time. Late submission/receipt of the Proposals shall not be entertained.

4.6. FORMAT FOR TECHNICAL BID

The bidders are requested to submit the technical proposal, which at least (but not limited to) shall include the following sections in the format provided below.

1. Executive Summary

2. Company Profile
3. Approach & Methodology for Proposed Consultancy and Managed Services
4. Assignment Management Strategy
5. Deliverables
6. Work Plan
7. Technical Team Composition with Certificates
8. Annexure - Evidence
    a) GST/NTN Certificate
    b) Organization's establishment and Affiliation with SECP
    c) Undertaking of Non-Black Listing on Rs. 100 Stamp Paper duly verified by Oath Commissioner/Notary Public
    d) Similar Assignments and References as per eligibility Criteria (Local and/ or International)
    e) Team Certificates & Resumes
    f) Organizational Financial Strength /Audited Statement

SECTION – V

5. GENERAL TERMS & CONDITIONS

5.1. BID SECURITY

A bid security is required and acceptable in the shape of a Bank Draft/Pay Order/Demand Draft/ Banker's cheque/CDR/Cashier Cheque only, issued from any scheduled bank operating in Pakistan, of rupees one hundred thousand (PKR 100,000/-), in the favour of CDNS, Islamabad. **The Bid Security must be submitted with the SEALED TECHNICAL PROPOSAL, without which the proposal shall not be entertained/ accepted.** If a bidder withdraws its bid during the procurement process or a successful vendor fails to acknowledge the letter of acceptance/signing of agreement etc.; in such scenarios the Procuring Agency reserves the right to forfeit the Bid Security besides considering other necessary actions under the law of the Land. Further the Procuring Agency may ask the second Most Advantageous bidder for award of contract and so on (as per its convenience) if the Most Advantageous bidder fails to comply. The bid security of unsuccessful bidder(s) may be released after contract signing with successful bidder. The bid security of successful bidder may be released after signing of the agreement and provision of the Performance Bank Guarantee.

5.2. VALIDITY OF PROPOSAL

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

5.3. PERFORMANCE BANK GUARANTEE. ("PBG")

The successful Bidder shall be required to submit an un-conditional and irrevocable ("PBG"), a sum equivalent to **05% (Five Percent) of** the total contract value (for the contract price of agreement to be signed with CDNS), valid for Three years. It has been observed that certain banks are not issuing the PBG for a continuous period of three years but for one year, in such case it would be the responsibility of successful bidder to submit the renewed PBG on yearly basis prior to expiry of previous PBG. Upon submission of renewed PBG, the previous PBG may be released. The ("PBG") shall be submitted on or before raising invoices. This ("PBG") shall be issued by any scheduled bank operating in Pakistan and the value for the outstanding deliverables of the contract will remain valid until the final and formal termination of Contract by Procuring Agency. The Procuring Agency may forfeit the ("PBG") 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 vendor/ company or any other action taken under the law or all or waive off all or partially based on sound justification that may be beyond its normal control, provided by the vendor and up to the satisfaction of procuring agency but the decision in this regard would be the sole discretion of the procuring agency and in no way, the vendor may consider it as its Right.

5.4. CURRENCY

All currency in the proposal shall be quoted in Pak Rupees (PKR) only otherwise bids would be rejected.

5.5. WITHHOLDING TAX, SALES TAX AND OTHER TAXES/LEVIES

The bidder is hereby informed that the Government shall deduct tax/duties at the rate prescribed under the tax laws of Pakistan, from all payments for services rendered purchase/supply by any bidder who signs the contract with the Government. The bidder will be responsible for payment of all taxes/duties on transactions and/or income, which may be levied by government till the date of submission of bid. In case of change/variation in rate of already levied taxes / duties been applied from the government after the date of submission of bid, such variation/change shall be applicable to the successful bidder.

It is pertinent to mention here that all new taxes/duties applied after the bid submission date shall be borne/paid by Procuring Agency

5.6. CONTRACTING (SIGNING OF AGREEMENT)

The selected Bidder shall submit draft Contract, for which specimen template may be obtained from procuring agency, and be signed on a stamp paper of Rs. 5000/- (which shall be notarized properly) immediately after issuance of work Order/letter of acceptance.

5.7. GOVERNING LAW

This RFP and any contract executed pursuant to this tender/RFP 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 the Courts at **Islamabad only.**

5.8. DISCLOSURE/ INTEGRITY PACT

Service Provider 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 Service Provider 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 Service Provider 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 Service Provider accepts full responsibility and strict liability for making and 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, Service Provider 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 Service Provider 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.

5.9. 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.

5.10 GRIEVANCE REDRESSAL

Any bidder feeling aggrieved by any act of the Procuring Agency after the submission of his bid may lodge a written complaint concerning his grievances not later than fifteen (15) days after the announcement of the bid evaluation report to the Grievance Redressal Committee of Procuring Agency. The Committee for the purpose is already notified at PPRA Website.

5.11 AMICABLE SETTLEMENT

5.11.1 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.

5.11.2 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 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.

SECTION – VI

6. BID ELIGIBILTY EVALUATION AND ACCEPTANCE CRITERIA

6.1. ACCEPTANCE CRITERIA

As per PPRA Rule 36(b) - Single Stage-Two envelope procedure, the proposals will be evaluated technically first. The Technical and Financial Proposals shall be allocated 60 and 40 marks, respectively. In Evaluation of Technical Bids 42 out of 60 marks are the qualifying marks. Financial bids of only technically qualified bidders will be opened. The distribution of 100 marks and formulae of financial bids evaluations will be as follows.

Technical Proposal (T) = 60 Marks. (42 are qualifying marks)

Financial Proposal (F) = 40 Marks.

Total (T+F) = 100 Marks.

The technical proposals/bids securing 42 marks i.e. 70% of total marks (60) allocated for Technical Proposals or more in the technical evaluation will qualify for the next stage, i.e. financial bid opening. The bidder whose quoted prices are lowest will get the maximum marks (i.e. 30 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 40 = Financial marks of (b)

The cumulative effect of both Technical and Financial marks shall determine the position of the bidders.

The contract may be awarded to the bidder(s) whose bid is approved on the basis of evaluation to be **"Most Advantageous Bid"** as per PPRA Rules.

Note: - The proposal from any firm which is blacklisted from any government entity will not be considered.

The Procuring may ask a bidder or all bidders to present/demonstrate CDNS HQ, Islamabad, their proposed methodology/ strategy to execute the entire assignment for CDNS, at their own cost and risk.

6.2. RESPONSIVENESS TEST/INITIAL SCREENING

Prior to the Technical Evaluation of the Technical Bids, All the Technical Bids shall be examined for the responsiveness Test/ Initial Screening based on following parameters/criteria which are pre-requisites and be considered as must meet requirements; non-compliance of any of following clause/parameter/criteria shall disqualify the bidder(s) straight away. All bidders are required to submit compliance sheet/page containing the Reference Page # in Technical Bid of proof.

6.2.1 The bidders must be registered with Taxation department and are on Active Taxpayer List for NTN/GST.

6.2.2 The Bidder should have minimum average annual turnover of Rs. 50 M for the last three years and are required to submit the valid proof to this effect. e.g audited financial statements for this period or any other evidence.

6.2.3 Affidavit on stamp paper (original and latest) of Rs.100/- signed by bidder and duly attested by Oath Commissioner/Notary Public, describing that bidder is not blacklisted from any government department and no suit is pending against the bidder(s) in any court of law.

6.2.4 Bid Security as an earnest money of required amount and shape, placed in the sealed Envelope of **Technical Proposal/Bid**.

6.2.5 Bidder must be registered with SECP or FBR in Pakistan at-least 5 years up-till the tender closing date. SECP or FBR Certificate to be provided

6.2.6 Bidding Company must have office in Pakistan. Proof of registered offices over the letter head to be attached.

6.2.7 The bidder must have performed at-least two(02) ISO 27000 Family Implementations Support either locally or international.

6.2.8 The Bidder must have design and Support at-least five (05) Penetration Testing projects in complex (either local or international) environments.

6.2.9 The bidding firm must have team of subject matter expert with IT security program design, implementation, readiness, assessment (i.e. Information security, HIPPA, ISO, SOC), and assurance experience with national and international projects of similar scope size and nature.

6.2.10 Company must be in information security consultancy and assessment business for at least the last five (05) years (in Pakistan). Proof to be attached such as IS assessment (any PO /evidence related to activities/tasks relevant to this RfP) etc.

6.2.11 Mandatory relevant domain experts with certifications in any of the applicable domains such as CISA, CDPSE, CISM, CEH, HIPPA.

6.2.12 The No objection Certificate (NOC) is required on bidders letter head duly signed and stamped by its authorized person stating that “We understand that Procuring Agency has published the Detailed Technical Evaluation criteria through clause 6.3 of this RFP and total marks allocated for Technical Evaluation. We have no objection and will never ask about the individual criteria wise marks to be published or shared with us.” Date, Name of authorized person, designation, signature, CNIC No. and stamp of bidding firm be mentioned on NOC letter.

Note: After closing date and time no bid will be entertained.

If any of the above mentioned mandatory mentioned criteria is not fulfilled, then the proposal will not be evaluated further.

If a bidding firm has fulfilled all the above-mentioned requirements, then the technical proposal will be further processed as per Technical Evaluation Criteria as mentioned in Clause 6.3 below:

6.3. TECHNICAL EVALUATION CRITERA (60 MARKS)

Key Characteristics		Max Marks	Remarks
I. Experience of Firm		**25**	
1	Bidder's team should have executed Information Security Assessments & Implementation projects (either Locally or Internationally)	5	Please provide necessary evidence
2	Number of Years in the Business	5	Copy of SECP / FBR Registration Certificate be provided
3	The bidder must have been awarded at least 2 national level IT security advisory projects.	5	Proof to be submitted
4	The vendor must have facility / its own open and fully customizable IT performance monitoring, security monitoring and IT risk management tools along with in house SecOps capabilities.	5	Please provide necessary evidence
5	Bidder must have experience to provide consultancy/advisory services and managed services related to information and cyber security to at least one financial institute / banks in Pakistan	5	
II. Project Professional Team		**10**	
Team Lead	Qualification: Masters/ higher education in Information Security/ Computer/IT/Networks or Bachelors in Computer/IT/Networks	05	
	Experience: 1. Must have executed at-least 3 information security audits either in Pakistan or international 2. Must have IT industry experience locally/globally of over 10 years (CV to be provided)		
Team Members	Bidder must have at least 3 SecOps/DevOps and Information security experts in their team having experience of atleast 5-10 years in IT Audits & Implementations either locally or internationally. CVs should be provided of at-least 3 resources along with their certifications who will be involved in the project. Bidder Team to have: i. Any one or more of the following Security Certifications in CISA/CISSP/CDPSE/HIPPA ii. 2 Years' experience in DevOps which is mandatory for the resource	05	

III. General Experience		**15**	
1	Bidder must be engaged in consulting/managed services role with minimum 3 deployments in Pakistan	3	
2	Bidder must have managed/deployed SOC and/or NOC services experience with national level organizations.	6	
3	Bidder must have 5 years of IT security monitoring and/or SEIM product SecOps/DevOps, NOC and SOC managed service offerings, and IT risk services (i.e. assessment, assurance and management).	6	
IV.	**Financial Strength**	**10**	
1	Financial Statement for the last three years with minimum average annual turnover of Rs. 50 M for the last three years. [2019, 2020 & 2021]	10	

Note:

i. **Submission of verifiable documentary proof for all above requirements and criteria points are mandatory requirement and marks will be awarded on the basis of these verifiable proofs. Every document to be duly signed and stamped by the authorized representative of the company.**

ii. **It is pertinent to mention here that in case of replacement of any resource [as mentioned/given in the technical bid], the successful bidder shall be responsible to provide the resource with same credentials/ experience and certification, in case of non-compliance of the same procuring agency reserves the right to terminate the contract with immediate effect.**

iii. **An eligible bidder, based on conditions listed in this document, not meeting the 70 % pass marks limit will be rejected in Technical Evaluation, and its sealed/unopened Financial Proposal shall be returned unopened. All bidders' technical proposal scoring greater than or equal to 70 % of the marks as mentioned in Clause 6.1 will be accepted and their financial bids will be opened**

Annexure – A

1.1. Resident Engineer 1

1.1.1. Information Security:

1.1.1.1. The Resident Engineer will be responsible for protecting CDNS IT infrastructure i.e. computers, networks and data against threats, such as security breaches, computer viruses or attacks by cyber-criminals.

1.1.1.2. Provide leadership, direction, management, and execution of all aspects of information security support to technology and the wider business

i. Responsible for envisioning and implementing the information security program

ii. Develop, implement and maintain Information security frameworks, policies, standards, guidelines and operating procedures. Ensure compliance with applicable regulatory requirements and industry practices

iii. Identify and prioritize strategic information security initiatives and associated financial investments

iv. Develop and implement third-party security assurance programs

v. Develop and implement security training and awareness programs. Educate staff members of all levels, including senior management, about potential security risks, the likelihood of those risks, costs, and effectiveness of possible remedies

vi. Define information security policies, processes and best practices across business units that establish clear guidelines for handling security matters and managing risk

vii. Evaluate information security and technology risk and integrate with risk management processes

viii. Provide information security direction and advice to business and technology projects as required

ix. Advise on the design, implementation, and maintenance of specialized hardware and software that secures the information technology environment

x. Ensure that applications are appropriately secure and aligned with corporate security standards

xi. Develop and implement an ISMS based on ISO 27001. Responsible for implementation and compliance with ISO 27001

xii. Identify and define gaps in security technology environment and advise on appropriate operational or technology required to address those gaps

xiii. Interface with internal and external auditors, regulators, Legal /Compliance and senior management on security matters

xiv. Establish and maintain activities and procedures to monitor the environment for suspicious activity or threats

xv. Define and implement escalation processes to identify and review critical security incidents, issues, and anomalies

xvi. Assist in the coordination of responses to security incidents

xvii. Advise the business on appropriate best practices to address information security related findings of internal and external audit reports

xviii. Train & oversee personnel with significant IT security duties

xix. Strengthen monitoring mechanism and controls especially from cyber threats

xx. Responsible for envisioning and implementing the information security program

xxi. Any other task assigned by CDNS

1.1.2. Background / Qualifications:

i. Graduation in Computer science, Information technology or equivalent from University/ Institution/ Board recognized by the HEC

ii. Certifications or course completion in the field of IT security will be preferred

iii. 5 years of experience in IT security and services in banking.

iv. Understanding of, and practical experience of applying the Data Protection Act, the Freedom of Information Act and other related legislation, standards and codes of practice

v. A good working knowledge of Information Security including ISO/IEC 27001 Information Security Management Standard

vi. Ability to lead and deliver change and contribute to culture change successfully

vii. Ability to influence at senior levels on matters relating to security and information risk

viii. Strong IT Infrastructure Domain knowledge

ix. Good Problem-Solving skills.

x. Decision making ability

1.2. Resident Engineer 2

1.2.1. Information Security:

1.2.1.1. The Resource is to review and enforce compliance with standards or regulations imposed by professional organizations or even a CDNS internal guidelines. Resource might conduct audits in areas of accounting, finance, information technology or security.

i. Responsible for development and implementation of IT self-assessment frameworks, compliance and with local and international best practices, internal policies and procedures, management of internal and external audit lifecycle

ii. Responsible for developing, maintaining and ensuring compliance with the enterprise architecture

iii. Ensure compliance with organizational frameworks, policies, standards, applicable regulatory requirements and industry practices

iv. Responsible to create audit mechanism and processes working with CDNS post digitalization of the organization

v. Engage auditees and other business stakeholders in a way that inspires and builds trust, mutual understanding, and respect

vi. Design and execute Audits, which utilize a range of risk-based assurance techniques

vii. Identify technical issues & vulnerabilities, assessing control gaps, and translate these into meaningful business risks.

viii. Deliver timely and meaningful audit outputs in alignment with the Core Audit Process (or other assurance products as required)

ix. Connect auditees and other business stakeholders to insights and resources that will deepen their understanding of risk and the internal control framework.

x. Anticipate and effectively manage potential obstacles to audit delivery

1.2.2. Background / Qualifications:

i. Graduation in Computer science, Information technology, Management information system, Accounting, Finance, business or equivalent from University/ Institution/ Board recognized by the HEC
ii. Professional license of (CISSP, CISA, CISM, CRISC, CISSP, ITIL, or similar) will be preferred.
iii. Minimum 4 to 5 years of experience in IT security or relevant field.
iv. Proficient in auditing: applications, distributed platforms (Windows/Unix), database (SQL/Oracle), infrastructure, and IT security tools and techniques
v. Ability to effectively manage information and communicate at all levels of the organization. Excellent verbal and written communication skills
vi. Experience with audit software and advanced data manipulation tools (ACL/Tableau) preferred
vii. Understanding of, and practical experience of applying the Data Protection Act, the Freedom of Information Act and other related legislation, standards and codes of practice
viii. Ability to influence at senior levels on matters relating to security and information risk
ix. Good Problem-Solving skills and Decision-making ability

1,1,3 Technology Infrastructure

- Lead the technology infrastructure and execution for CDNS
- Planning and implementation leadership, identifying opportunities for automation, cost savings, and service quality improvement
- Provide infrastructure services vision, enable innovation and seek to leverage IT trends that can create business value consistent with CDNS technology requirements and expectations
- Develop enterprise standards and technology architecture and the IT operations governance process
- Conduct product and vendor evaluations ensuring best-in-class technologies and partners
- Work closely with and manage strategic vendor partner relationships
- Hands-on technical depth to enable direct oversight, problem-solving leadership and participation for complex infrastructure implementation, system upgrades and operational troubleshooting
- Experience with comprehensive disaster recovery architecture and operations, including storage area network and redundant, highly-available server and network architectures
- Leadership for delivery of 24/7 service operations and KPI compliance
- Determine appropriate SLA levels with relevant external stakeholders. Ensure that the infrastructure is in place to meet those SLAs. Measure performance against those SLAs
- Manage, lead and direct teams involved in network and infrastructure support, and infrastructure projects. This includes implementation of strategic infrastructure projects, establishment and management of data and voice networks (WAN/LAN/ADSL) and computing infrastructure and facilitation of the delivery of information services and projects
-

Skills

- Experience of leading overall infrastructure for a complex organization and network, including VLAN setup for regulatory requirement, managing data protection, etc.
- Working knowledge of Storage Area Network (SAN) and related technologies, network communications technology, high availability and disaster recovery architecture, communication and related technologies
- Experience with regulatory compliance issues, as well best practices in application and network security
- Must have industry experience in the specific areas mentioned above with conventional financial service providers (e.g. banks) clients or with digital financial service providers (DFSP) clients in the private sector
- Desired professional certifications in the area of data center certifications (e.g. Cisco, Juniper, VMware), network certifications (Cisco, Juniper), Linux / Unix Sys Admin, cloud computing (nice to have), ITIL certified

Qualification

- Minim um Bachelor's degree in information technology or computer sciences or related disciplines from a reputable and recognized local or international university
- Minimum 7 years of 'vendor/ infrastructure management' experience in one or more of the following areas: LAN and WAN, data center relocation or managed services, data and voice networks, network security, network administration, operating systems, databases, disaster recovery, capacity and availability monitoring

- ITIL certified

1.1.4 System Administrator

responsible for managing, troubleshooting, and proactively updating hardware and software assets to prevent downtime or zero-day exploits from occurring

- Plan, install, configure, troubleshoot, and administrate Windows and Linux Server based operating environment and its related services, including but not limited to IIS, domain implementation, update server implementation, Active Directory implementation
- Perform process automation, scheduling tasks, shell scripting, etc.
- Create an understanding of CDNS's networks, databases, internal and external systems
- Develop, deploy and monitor CDNS internal and external system, and other system-oriented projects
- Apply reporting tools for IT infrastructure, servers, SAN, CCTV, access control devices etc. and provide reports and documents as per CDNS requirements
- Ensure availability and optimal performance of CDNS systems throughout the year
- Responsible for implementation of back-up and restore methodologies of CDNS, developing disaster recovery (DR) site engagements ensuring business continuity of CDNS
- Manage and maintain SOPs formulation, policy deployments, operational documentations
- Perform custom installation, customization on already installed servers, change the defaults, harden the server
- Implement server level layered security approach
- Patch or upgrade the operating system for clients and servers as required

Implement firewalls, IDS administration and troubleshooting

SKills

- Proven experience in deploying, configuring, troubleshooting administrating and monitoring of different services hosted on UNIX like operating systems (like LINUX etc.)
- Hands on expertise on virtual environment deployment, its operational issues, monitoring aspects along with migration of VMs, their snapshots, backups, etc.
- Must know the "defense in depth" concept of layered security approach
- Must know the basic security concepts and cyber attack techniques/ terminology like TCP vs UDP communication, DoS, DDoS, Phishing, Trojon/ malware, spoofing, flooding, encryption of data at rest, on transit and on backup, man in the middle, firewalls, intrusion detection and prevention, data leakage prevention, WAF, routing, etc.

Qualification

- Proven experience in deploying, configuring, troubleshooting administrating and monitoring of different services hosted on UNIX like operating systems (like LINUX/SOLARIS/AIX etc.)
- Hands on expertise on virtual environment deployment, its operational issues, monitoring aspects along with migration of VMs, their snapshots, backups, etc.
- Must know the "defense in depth" concept of layered security approach
- Must know the basic security concepts and cyber-attack techniques/ terminology like TCP vs UDP communication, DoS, DDoS, Phishing, Trojon/ malware, spoofing, flooding, encryption of data at rest, on transit and on backup, man in the middle, firewalls, intrusion detection and prevention, data leakage prevention, WAF, routing, etc.

Annex-B

No Objection Certificate (NOC)

-Print on letter head of bidding firm/company-

Director General
Central Directorate of National Savings,
23-N, Melody Market, G-6 Markaz,
Islamabad.

Subject: **No Objection Certificate (NOC)**

Sir,

Reference to clause # 6.2.12, We, M/s_____ understand that Procuring Agency has published the Technical Evaluation criteria through Article 6.3 of this RFP and total marks allocated for Technical Evaluation. We have no objection, and we will never ask about the individual criteria wise marks to be published or shared with us

We look forward to your favourable response.

Regards

(Name of authorized person)
(Designation)
(Signature)
(CNIC#)
(Stamp of firm/ company)

FINANCIAL BID FORMAT

S#	Activity / Scope	Monthly cost / service charges (PKR) (without taxes)	Monthly cost / service charges (PKR) (With all applicable taxes)	Total cost / service charges (for Year - 1 (PKR) (With all applicable taxes)	Total cost / service charges (for Year - 2 (PKR) (With all applicable taxes)	Total cost / service charges (for Year - 3 (PKR) (With all applicable taxes)	Total cost / service charges (for Year - 4 (PKR) (With all applicable taxes)	Total cost / service charges (for Year - 5 (PKR) (With all applicable taxes)
1	Year - 1 Information Technology and Information Security Governance				N/A	N/A	N/A	N/A
2	Year - 1 Secure coding Platform and services of Core banking Application (Lump Sum Cost be required)	N/A	N/A		N/A	N/A	N/A	N/A
3	Year - 2 Implementation governance of Year1 scope			N/A		N/A	N/A	N/A
4	Software, Tools, Solutions, Licenses, HW to establish SOC			N/A				
	Management of SOC operations.			N/A				
5	Software, Tools, Solutions, Licenses, HW to establish NOC			N/A				
	Management of NOC operations.			N/A				
6	VAPT (Bi-Annually) i.e. 4 times over the period of 3 years							
7	Training						N/A	N/A
Total Cost / Service charges (PKR with all applicable taxes) [S # 1 - 7]								
8	Information Security							
	Information Security							
	Technology Infrastructure							
	System Administrator							
Total Cost / Service charges (PKR with all applicable taxes) [S # 8]								
G. Total Cost / Service charges (PKR with all applicable taxes) [Total of S # 1-7] + [Total of S # 8]								


National Savings
Ministry of Finance
Government of Pakistan
SAVINGS HOUSE
NATIONAL
SAVINGS