Request for Proposal for
Comprehensive IT Services Management

Department of Information Technology

National Bank for Agriculture and Rural Development (NABARD)
Department of Information Technology
5th Floor, 'C' Wing C-24, 'G' Block
Bandra Kurla Complex, Bandra (East)
Mumbai - 400051
Maharashtra
Ph: 022-26539667

Important Disclaimer:

This Request for Proposal (RFP) is not an offer by NABARD, but an invitation to receive response from eligible interested bidders for the IT Services Management. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by NABARD with the Bidders. This document should be read in its entirety.

Table of Contents

APPENDIX

1. Critical Information

National Bank for Agriculture and Rural Development (NABARD) invites e-Bids from prospective bidders. Interested Bidder must submit relevant documents in https://nabard.eproc.in. The Bidder shall submit two separate Bids for the service (Technical Bid and Commercial/Financial Bid).

<table>
<tr><td>Tender Reference No and Date</td><td>No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022</td></tr>
<tr><td>Tender For</td><td><b>Comprehensive IT Services Management</b></td></tr>
<tr><td>Cost of RFP (Non-Refundable)</td><td>No cost will be charged for the tender document downloaded by the bidders. Rs.1000/- (Rupees One Thousand Only) in the form of DD in favour of NABARD payable at Mumbai should be deposited if Hard Copy is to be supplied.

In terms of Public Procurement Policy for Micro and Small Enterprises (MSEs) Order 2012, the MSEs registered with National Small Industries Corporation under Single Point Registration Scheme for participation in Government purchases, shall be exempt from payment of cost of tender documents. Further, the vendors empanelled with the Bank will also be supplied tender documents free of cost. However, they will have to produce documentary evidence in support of seeking such exemption.</td></tr>
<tr><td>Earnest Money Deposit (Refundable)</td><td>Remittance of Rs. 10,00,000/- (Rupees Ten Lakh Only) to NABARD's Account. The UTR No for this transaction has to be indicated in the Bid Document.

<table>
<tr><td>Name of Account</td><td>NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT</td></tr>
<tr><td>Bank Name</td><td>NABARD</td></tr>
<tr><td>Branch Name</td><td>HEAD OFFICE, MUMBAI</td></tr>
<tr><td>IFS CODE</td><td><b>NBRD0000002</b></td></tr>
<tr><td>Account Number (VAN)</td><td>NABADMN07</td></tr>
</table>
<b>OR</b>
Bank Guarantee of an equivalent amount issued by a Scheduled Commercial Bank valid for 180 days from the date of opening of tender as per format given in Annexure-IV.</td></tr>
<tr><td>Date of Issue of RFP</td><td>12-05-2022</td></tr>
<tr><td>Last date for submission of pre-Bid queries</td><td>27-05-2022 at 18:00 hours
All queries should be sent to dit@nabard.org with cc to pravesh.gangwar@nabard.org</td></tr>
<tr><td>Date of Pre-Bid Meeting</td><td>31-05-2022 at 14:00 hours</td></tr>
</table>

Reply to pre-Bid queries	15-06-2022
Last date & time for submission of Bid	27-06-2022 at 15:00 hours
Opening of Technical Bid	27-06-2022 at 15:30 hours
Opening of Commercial Bid	Will be intimated to shortlisted bidders at a later date.
Opening of tenders	e-tendering at https://nabard.eproc.in
No. of e-bid documents to be submitted online	**Technical Bid:** Including Cost for RFP Document + EMD (UTR No. & date/BG) + Documents as per Check List +**Commercial Bid**
Contact Numbers	Shri Pravesh Gangwar, Manager 022-26539667, +919599773516
Email	dit@nabard.org, pravesh. gangwar @nabard.org

2. Introduction and Disclaimers

2.1. Purpose of RFP

2.1.1. The National Bank for Agriculture and Rural Development hereinafter called "NABARD" or "Bank" or "Purchaser" or "Buyer" issues this 'Request for Proposal, hereinafter called "RFP" with the purpose to engage service provider for IT Services Management(ITSM) as per Scope of work and Technical Specifications etc. given in this RFP.

2.1.2. Bank intends to procure the IT Service Management (ITSM) and IT Asset Management (ITAM) solutions along with commissioning, installation, implementation, maintenance, monitoring & management etc., which include modules like Ticketing processes,Process flow Management,Capacity Management, Server management, Database Management, Storage Management, Configuration management, Patch Management Solution, Inventory Management Solution, Network Management and Automation Solution,HCI (Hyper Converged Infrastructure) Management, SDDC maintenance and management and clustered servers., Backup and Storage management, mNetworking, Firewall, NAC, Wi-Fi, ILL, MPLS, IFTAS and SDWAN maintenance and management, warranty support of all devices.

2.2. Parties to the RFP

The Parties in the RFP shall be referred as below:

2.2.1. "The Bank", "NABARD", "Purchaser", "Buyer" means National Bank for Agriculture and Rural Development (NABARD);

2.2.2. "Bidder", "ITSM Service Provider", "Supplier", "Service Provider", "Seller", "Recipient", "Respondent" means the respondent to the RFP document.

2.3. Information Provided

2.3.1. The RFP document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending bidder to determine whether or not to submit a response/bid or enter into a contract or arrangement with NABARD.

2.3.2. Each Recipient should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice.

2.3.3. Neither NABARD nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of this document.

2.4. Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by applicable law, NABARD and its directors, officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of NABARD or any of its officers, employees, contractors, agents, or advisers.

NABARD may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. NABARD has the right to continue with these activities, modify the sequence of activities, add new activities, or remove some of the activities, as dictated by the best interests of NABARD. NABARD reserves the right to reject all or any of the proposals without assigning any reasons whatsoever.

2.5. Costs to be borne by Respondents

All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including the attendance at meetings, discussions, demonstrations, presentation, visits etc. and providing any additional information required by NABARD, will be borne entirely and exclusively by the Respondent.

2.6. No Legal Relationship

No binding legal relationship will exist between any of the Respondents and NABARD until execution of a contractual agreement.

2.7. Recipient Obligation to Inform Itself

The Recipient must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

2.8. Errors and Omissions

Each Recipient should notify NABARD of any error, omission, or discrepancy found in this RFP document.

2.9. Acceptance of Terms

A Recipient will, by responding to NABARD for RFP, be deemed to have accepted the terms of this RFP including Introduction, Disclaimer and the schedules and annexures to the RFP. Deviations, if any, are to be specified as per Annexure X.

2.10. Requests for Proposal

2.10.1. Recipients are required to direct all communications related to this RFP, through the nominated point of Contact Person

Contact Person	Pravesh Gangwar	Rajee Murlidharan
Position	Manager	Assistant General Manager
Email ID	pravesh.gangwar@nabard.org	rajee.murlidharan@nabard.org
Telephone No.	022-26539667	022-26539171

2.10.2. NABARD may, in its absolute discretion, seek additional information or material from any of the Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent’s response.

2.10.3. Respondents should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RFP could be conveyed promptly.

2.10.4. If NABARD, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then NABARD reserves the right to communicate such response to all Respondents.

2.10.5. NABARD may, in its absolute discretion, engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

2.11. Notification

NABARD will notify all short-listed Respondents in NABARD website or by writing or by mail as soon as practicable about the outcome of the RFP process. NABARD is not obliged to provide any reasons for any such acceptance or rejection.

3. Background

3.1. About NABARD

National Bank for Agriculture and Rural Development is a body corporate established under the NABARD Act, 1981 (hereinafter referred to as “NABARD” or “the Bank” or “Purchaser” or “Buyer”) having its Head Office at C-24,'G' Block, Bandra-Kurla Complex, Bandra (East), Mumbai-400051 (hereinafter referred to as “NABARD Head Office”) and regional offices, training establishments and other setups in different cities across India.

The mission of NABARD is to promote sustainable and equitable agriculture and rural development through participative financial and non-financial interventions, innovations, technology, and institutional development for securing prosperity.

NABARD’s initiatives are aimed at building an empowered and financially inclusive rural India through specific goal-oriented interventions which can be categorized broadly into three heads: financial, developmental and supervision, touching almost every aspect of rural economy. From providing refinance support to building rural infrastructure, from preparing district level credit plans to guiding and motivating the banking industry in achieving these targets, from supervising Rural Cooperative Banks (RCBs) and Regional Rural Banks (RRBs) to help them develop sound banking practices and on-boarding them to the Core Banking Solutions platform, from designing new banking schemes to the implementation of Government of India’s (GoI) development schemes, from upgrading skill handicraftsmen to providing them a marketing platform for selling these articles, it touches millions of rural lives across the country. Detailed information regarding the functions of the Bank is provided on NABARD’s website www.nabard.org.

3.2. Subsidiary/Associate Organizations of NABARD

3.2.1. NABCONS : NABARD Consultancy Services (www.nabcons.com)

NABARD Consultancy Services (NABCONS) is a wholly owned subsidiary promoted by NABARD and is engaged in providing consultancy in all spheres of agriculture, rural development and allied areas. NABCONS leverages on the core competence of NABARD in the areas of agricultural and rural development, especially multidisciplinary projects, banking, institutional development, infrastructure, training, etc., internalized for more than two decades.

3.2.2. NABFINS : NABARD Financial Services (www.nabfins.org)

NABFINS is an initiative of NABARD born out of serious concerns about the practices of NBFC MFIs in the mid-2000. Entrusted with the responsibility of promoting microfinance sector besides scaling up SHG-Bank Linkage, NABARD thought it fit to form a Micro Finance institution on a pilot basis with the objective of developing it as a model NBFC in the country which will facilitate setting up of benchmarks and standards for the MFI sector. In particular, NABFINS objective was to ensure that the various maladies found in the NBFC MFI sector such as lack of transparency in accounting and disclosure, high transaction cost, lack of diversification in products, increased rates of interest, coercive collection practices etc. are sought to be eliminated by establishing a fair and transparent Micro Finance Institution.

3.2.3. NABKISAN : NABKISAN Finance Limited (www.nabkisan.org)

NABKISAN is a subsidiary of National Bank for Agriculture and Rural Development with equity participation from NABARD, Govt. of Tamil Nadu, Indian Bank, Indian Overseas Bank, Tamilnad Mercantile Bank, Canara Bank, ICICI Bank, Federal Bank, Lakshmi Vilas Bank and a few Corporates / Individuals. The company is notified as a Non-Banking Finance Company (NBFC) by RBI. The main objective of the company is to provide credit for promotion, expansion and commercialization of enterprises engaged in agriculture, allied and rural non-farm activities. NABKISAN is providing support for livelihood/ income generating activities by extending credit to Panchayat Level Federations, Trusts, Societies and Section 25 companies/ MFIs for on-lending to its member SHGs/ JLGs.

3.2.4. NABVENTURES Limited (www.nabventures.in)

NABVENTURES Ltd, incorporated by NABARD under the Companies Act, will provide early -stage support for agriculture and rural enterprises and fill the gap of adequate institutional support to them.

3.2.5. NABSAMRUDDHI Finance Limited (www.nabsamruddhi.org)

NABSAMRUDDHI Finance Limited was incorporated under Companies Act, 1956 on 17 February 1997 under the name of Agri Business Finance Limited (ABFL) and registered as Non-Banking Financial Company with the Reserve Bank of India. It is promoted with equity participation from National Bank for Agriculture and Rural Development, Andhra Bank, Canara Bank, Government of Andhra Pradesh, Government of Telangana, Andhra Pradesh State Cooperative Bank, Telangana State Cooperative Apex Bank and a few Industrial Houses / individuals from the State.

The objective of NABSAMRUDDHI is to provide credit facilities to individuals and legal entities for promotion, expansion, commercialization and modernization of enterprises and individuals engaged in non-farm activities including microfinance, MSME, housing, education, transport, etc.

3.2.6. NABFOUNDATION (www.nabfoundation.in)

NABFOUNDATION, a not for profit, wholly owned subsidiary of NABARD has been successfully incorporated on 31 August 2019 under Companies Act, 2013. NABFOUNDATION aims to emerge as a strong and vibrant institution so that other financial institutions, Government agencies and Corporates would avail its services for implementation of various development projects in the agriculture and rural sector.

3.2.7. NABSANRAKSHAN (www.nabsanrakshan.org)

NABSanrakshan Trustee Company Private Limited is a wholly owned subsidiary of NABARD with an authorised capital of ` 100 crore. NABSanrakshan aims to carry out credit guarantee and related activities towards sustainable and equitable agriculture and rural development. Agriculture and allied industry being a priority for the economy in creating new avenues for development, NABSanrakshan will provide the necessary fillip to the growth of the sector, through access to finance.

3.2.8. Please visit NABARD website (www.nabard.org) for complete list of subsidiary /associate organization of NABARD.

3.3. Current Setup

3.3.1. Data Center

NABARD has hosted its corporate Data Center (DC) on a Co-location model in Mumbai. While the datacenter facilities viz. DC cage, Racks, power, UPS, cooling, humidity controls, physical security, fire and safety controls etc. are provided, managed and maintained by the Datacenter Service Provider, the IT Infrastructure items hosted inside the DC Cage viz. Servers, Storage, Network and Security devices, Backup devices, LAN/ WAN etc. are owned, managed and maintained by NABARD or through its 3rd party managing partner(s). NABARD has also taken two seats at DC for seating of on-site ITSM resources. The DC houses almost all the applications currently used in the Bank including approximately 20 enterprise applications 30 other business applications. Few applications which are not hosted in DC are enroute to be hosted in DC in the near future. Currently, the DC comprises of 255 servers which includes 15 physical servers and the rest being logical / virtual servers. The DC also houses Software Defined Wide Area Network (SDWAN) technology through which it is connected to the other offices. Along with it, the DC also houses firewall for internet access. Apart from these, the DC is also equipped with San Storage devices and Tape Back-up devices. The DC corresponds to Tier-III DC standards.

3.3.2. Disaster Recovery Site

NABARD has a Disaster Recovery (DR) Site on a Co-location model in Faridabad, Haryana. All critical IT Services provisioned for delivery from DR.

3.3.3. Corporate Network

Our Bank has a Wide Area Network (WAN) through a MPLS cloud services from BSNL and a redundant service from M/s Airtel. Every RO of the Bank has its own local network (LAN) and 1-2 servers for their local needs. ROs have their independent internet connectivity. Further, all these LANs are connected to the WAN. All the centralized applications hosted in DC located at HO, can be accessed through the corporate WAN. Some of these applications can also be accessed through Internet.

At Head Office: HO LAN consists of about 900 devices. Logically this LAN comprises of 9 VLANs which are connected through Edge-room switches and core switches in a "Star" formation. Further, there are two 32 MBPS Internet leased lines (totaling 64 Mbps) for accessing Internet and providing Internet based services from our DC.

At Regional Offices: The LAN at ROs consists of all the devices of the RO. The size of the LAN depends upon the size of the RO. The bigger ROs have about 250 devices on their network. Further, each RO has an independent Internet Broadband line ranging from 1-2 MBPS as per their requirement.

3.3.4. Firewall for All Ros

At present, only HO LAN is protected by a perimeter level firewall. With the advent of MPLS based WAN, it is imperative that the LANs of all ROs should also be protected through a perimeter level dedicated firewall. Accordingly, Unified Threat Management (UTM) has been implemented across all ROs which is being managed and administered remotely from a central location in the HO.

3.3.5. Network Devices

Type of Device	Number of Devices	Remarks
SDWAN Device	34*2 + 4 = 72	2 at each RO & HO and 2 at DC & 2 at DR
Core Switches	34*2 + 8 = 74	68 in RO's and 2 at each DC, DR & Near DR in HO
Perimeter Firewall	4	2 at DC & 2 at DR
Firewall – UTM Internal	4	2 at DC & 2 at DR
NAC server	2	AT DC & DR
Wi-Fi -controller	40	HO
Wifi - Firewall	2	
Wifi - Switches	16	

3.3.6. Services

At present, NABARD has Centralized IT services like AMC for Computers and Peripherals at HO, RO and TEs FMS for Infra Domain Services, which includes Endpoint through single ITSM Service Provider (Tata Consultancy Services Limited (TCS)). Centralized ServiceDesk facility is available at NABARD Head Office to log ticket in Ticketing Tool for providing comprehensive IT Services

3.4. RFP Objective

3.4.1. Objective

i. NABARD intends to e the IT Services Management provider responsible for day-to-day operational requirements of commissioning, installation, implementation, maintenance, monitoring, updates, upgrades, replacements, troubleshooting & management of entire IT infrastructure

ii. The period of Contract would be 5 years from the execution of the Contract. This period of Contract may be extended by one year at the same cost as existing cost of 5th year.

4. Scope of Work

The scope of work includes the below mentioned:

4.1. Project Scope, Objective, and Goal

4.1.1. Objectives and Requirements

NABARD intends to engage the IT Service Management (ITSM) Provider responsible for day-to-day operational requirements of commissioning, installation, implementation, maintenance, monitoring, updates, upgrades, replacements, troubleshooting & management of entire IT infrastructure at NABARD including but not limited to the following activities and services:

4.1.1. IT Service Management

1. AMC for IT assets and Peripherals
2. Desktop Management using the centrally managed tool
3. Inventory Management using tool
    - Configuration management (system and devices configuration at DC/DR/HO/RO/TE) and any other location prescribed by Bank.
    - Ticket logging for warranty support of all devices.
4. Patch Management using tool
5. Domain Service Management (Active Directory, LDAP)
6. File Services Management
7. Storage Management
    - Storage Management (allocation, monitoring, troubleshooting)
8. Backup Management
    - Backup and Storage management (Arcserve & HPDP)
9. Data Center and Server Management
    - Server management (Maintain server log book, install, update, troubleshoot, tuning, monitor, auto alert, SSL installation, certificate based access), JBOSS Support, all native OS services of windows, linux, AIX, webservers
    - HCI (Hyper Converged Infrastructure), SDDC maintenance and management of clustered servers.

10. Network Management Services

- Network Management and Automation Solution, Support and co-ordination for IFTAS cloud

11. IT Security Management

- Networking, Firewall, UTM, NAC, Wi-Fi, ILL, MPLS, IFTAS and SDWAN maintenance and management. (e.g. Juniper, Fortinet, Forcepoint, checkpoint, sonicwall, etc)

12. Database Administration

- Database Management (install, update, fine tuning, replication, recovery, backup & restore, monitoring, auto alert)

13. Vendor Management

14. HelpDesk and Service Desk Management

- Ticketing processes (ticket logging, classifying, assigning, resolving, escalating), helpdesk and services.

15. General

- Process flow Management of all ITSM verticals.
- Capacity Management (Assigning, troubleshooting, alerting)

4.1.2. Scope involves the provisioning and management of mentioned ITSM requirements, based on the Bank's requirement as stated in the RFP.

2.1. NABARD would like to avail these services in a managed service model through a single ITSM Service Provider. All necessary tools, software's (All Licenses should be in name of NABARD) necessary for the administration and management of all the service components should be provided as mentioned in clause 4.1.1.

2.2. All the service monitoring and management tools must be deployed on-premises. Monitoring and Management Tools should be available to both onsite and offsite teams for delivery of these services.

2.3. Web based asset and inventory management tools with access for DIT users and management.

2.4. Option of API based integration with other applications should be available in asset and inventory management tool.

2.5. ITSM service provider should maintain onscreen display panel of ticketing and all devices/infra services dashboard.

2.6. The activities like capacity planning, architecture re-designing (for DC /DR/HO/RO and Network) etc. must also be provided for all the above services.

2.7. The scope of ITSM Service Provider contains support for the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches:

- Firmware/BIOS Upgrades / up to date patching,
- Faulty Parts replacement,
- Hardware System monitoring,
- Troubleshooting & Performance Tuning,
- Operating System Upgrades, antivirus and software upgrades,
- Upgrades of supplied software, all commonly used softwares
- Advisories on software upgrades & vulnerabilities
- DR Drills operations based on SOPs of Nabard.
- OS Administration & patching as per OEM guidelines
- VAPT Compliance/Audit /Review as per Bank's requirement /Statuary guidelines
- Any support required to make system & solution up and running as per SLA.

2.8. The ITSM Service Provider should keep the bank explicitly informed about the end of support dates of the related products/hardware and should ensure support during the warranty and AMC period.

2.9. The ITSM Service Provider should provide the complete documentation including technical, operations, user manual, design documents, process documents, technical manuals, functional specification, system configuration documents, system/database administrative documents, debugging/ diagnostics documents, test procedures etc.

2.10. The ITSM Service Provider shall formulate/ supply/share all kinds of procedures/ documents upon any level or version changes, clarification, corrections and modifications in the above-mentioned documents on each incident of change.

2.11. ITSM Service Provider requires to install and configure Comprehensive Monitoring of End-to-End IT Services (Network, Server, Storage, Appliance, Database and Applications across all locations of the Bank)

2.12. The ITSM Service Provider shall implement Active Directory Certificate Services (AD CS) to create Public key infrastructure in the bank environment to underpin identity and other security functionality on windows domain so that it can create, validate and revoke public key certificates for internal uses of the organization. The ITSM Service Provider shall do end to end management of Active Directory System of the Bank for all services.

2.13. The ITSM Service Provider shall ensure end to end completion of all activities initiated as part of the project. The ITSM Service Provider shall coordinate with other stakeholders also for completion of activity.

2.14. The ITSM Service Provider shall migrate all the data from existing ITSM and IT Asset Management tools to new tool.

2.15. The ITSM Service Provider shall provide the details of all tools/softwares they will be using for ITSM service management, ticketing, monitoring, inventory management, patch management, os installation, desktop support tool etc.

2.16. The ITSM Service Provider shall provide user logins for DIT staffs on all tools/software used for ticketing, monitoring, inventory management, etc.

2.17. The ITSM Service Provider will have to handover the system in 100% working condition on termination or at the end of the contract. Any breakdown call that has been reported before termination of the contract shall have to be corrected by the ITSM Service Provider before handing over to Bank.

2.18. The Bank can terminate the contract with Service Provider and discontinue the same due to performance issues by giving 90 days' notice.

2.19. Contract can be extended at the discretion of the bank at the same rate for last service year after the expiry of the contract period.

2.20. The Bank, at its sole discretion, will enter into AMC for IT assets.

2.21. Bank at its discretion can terminate the contract in whole or as part thereof with the ITSM Service Provider and discontinue the same without citing any reason by giving 90 days' notice or applicable amount, on a pro-rata basis.

2.22. Submission of periodical reports on the performance of the equipment's and its reviews. Preparation and submission of other MIS related work assigned by the Bank.

2.23. A suitable mechanism for setting priority for critical events on the basis of service impact and user groups (VIP users) should also be provided for all these services.

2.24. The ITSM Service Provider shall ensure regular backup as per the backup policies of NABARD and its restoration as and when required by the bank with appropriate permissions. Proper check of restorability of backup media needs to be carried out periodically as defined by the bank.

2.25. Preparation of SOP of all verticals for all existing and new services from the day 1 (one) of service contract.

2.26. Periodic Review all SOP

2.27. ITSM service provider should ensure pay the higher minimum wages between central and states governments and other statutory guidelines as applicable during the period of contract. Service provider should submit necessary certificates to NABARD in this regard.

2.28. Manage operations for all upcoming cyber security solutions i.e. IAM (Identity and Access Management), DAM (Database access management), Brand Monitoring Solution, DNS security, Patch Management, Vulnerability Management, DLP(Data Leak Prevention), security and any other solution.

3. Detailed Requirements

3.1. Annual Maintenance Contract (AMC)

3.1.1. As and when NABARD acquires new IT asset(s) after the start of this contract, coordination and timely closure of warranty and extended warranty related requirements for all IT assets. If on expiry of essential warranty/extended warranty, NABARD decides to enter into AMC of assets such as Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanner with ITSM service provider, rate for the same will be determined based on the unit rate already decided for the existing item in AMC.

3.1.2. The type of maintenance will be fully comprehensive on-site including repair /replacement of parts and if not repairable, ITSM will inform NABARD within 7 days. Maintenance Services shall consist of preventive and breakdown maintenance of Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanners.

3.1.3. A rate card will be part of quote based on SOP for attending to complaints within 48 hours for all district/cluster offices of the bank.(Rate card annexure).

3.1.4. If 'End of Service Life' (as mutually agreed between NABARD and the Service Provider) of an asset falls in between any quarter during contract period, Service Provider will intimate NABARD at least 90 days in advance for replacement of the same. However, Service provider shall continue to provide AMC and ITSM support for these items till NABARD replaces them with new items.

3.1.5. At any stage of the contract, NABARD reserves the right to terminate the AMC for any of the item(s), with due prior notice of 30 days to the service provider. Service provider shall raise invoices for all the subsequent quarters after deducting the AMC charges for the items taken out of AMC.

3.1.6. The current timings for providing AMC services are given below. It is possible that these timings may change in future, but the total working hours will be 9 hours on weekdays.

Working Day	**Time From**	**Time To**
Monday to Friday	9.00 am	6.00 pm (or as required)
Saturday/Sunday/Holidays	As required	As required*

*At no additional cost

Online attendance portal access should be provided by ITSM service provider to DIT management for all their staff including subcontractors along with daily email of attendance sheet at 9:15 AM.

3.1.7. The service segment can be split, if need be, into critical and non-critical services for the purpose of round-the clock on-site monitor.

3.1.8. The complete inventory of all the IT Assets / Equipment which are to be managed and services are given in the **Appendix IV**

3.1.9. The Service Provider will have to provide support for all computer hardware, software and network related calls as logged by NABARD. Service Provider will be responsible for troubleshooting and resolution of related calls and report them back to Central Helpdesk.

3.1.10. The Service Provider will undertake to maintain highest service standards as per good industry practice. The Service Provider will arrange for qualified and experienced resident engineers to meet the above-mentioned service levels. For successful implementation and smooth functioning of the operations, personnel with appropriate skills, aptitude and experience would be deputed at NABARD offices. Service Provider shall submit resumes of engineers to be deployed at NABARD. NABARD would have the right to accept / reject the proposed personnel. Also, if any personnel were to quit then handholding would be necessary with suitable replacement with prior notification to NABARD.

3.1.11. The Service Provider will provide on-site maintenance services. Service Provider should provide PC/Printer/Notebook Computer/Networking equipment in case the problem is not resolved within 4 working hours for the concerned user to carry out his day-to-day work from buffer stock of NABARD. ITSM Service Provider shall provide all essential tools, service kit and testing toolkit needed for maintenance of the computer systems at all locations.

3.1.12. The ITSM Service Provider shall conduct preventive maintenance as may be necessary from time to time (minimum twice in a year) to ensure that equipment is in efficient running condition to ensure trouble free functioning.

Preventive maintenance Scope

a. Physical cleaning using blower.
b. Bios updates.
c. OS and antivirus patch updates.
d. Software updates.
e. Inventory update
f. Any other related activity

3.1.13.. The ITSM service Provider shall conduct physical verification of assets minimum once in a year or as need arises.

3.2. Desktop Management using the tool

The ITSM Service Provider should be capable of installation, configuration and using the tool and perform the following activities:

3.2.1. Taking control of remote desktops using tool.

3.2.2. Remote Management of Desktops - installation, configuration and troubleshooting of operating system, Anti-virus and all user Applications in the desktops/laptops.

3.2.3. Remote installation of patches

3.2.4. Remote Routine maintenance of PCs (e.g., cleaning up file system debris, defragmenting drives, running malware scans, etc.)

3.2.5. Taking back-up while configuring new systems.

3.2.6. Guide and direct users to relevant desk/department/individuals in case support required is not under scope of deliverables by the ITSM Service Provider and carrying out related activities.

3.2.7. Use latest technology for bulk installation for multiple machine.

3.2.8. Special Note: Desktop management services are required to be provided for IT equipment (i.e. PC/AIO, Printer, Laptop, Scanner, Internet etc.) at the residences of senior executives (CGM/OIC and above) at all locations and KVS, Dadar.

3.3. Inventory Management using tool

The ITSM Service Provider should perform the following activities:

3.3.1. Capable of installation, configuration and using the tool (import of existing data).
3.3.2. Should maintain the Catalog of software and hardware from all major OEMs/Principals and should update the signature for the same on periodic basis. The update periodicity should be as per industry norms.
3.3.3. Managing Configuration Management data base (CMDB).
3.3.4. Initially, complete inventory of all IT assets in the Bank has to be taken up independently with relevant tools and the same has to be shared with the Bank and later on periodicity as decided by bank.
3.3.5. Dashboard to identify the addition and deletion of IT assets in the Bank for custom period.
3.3.6. Capable of Configuration item (CI) identification, planning and controlling configuration changes
3.3.7. Capable of configuration change report generation
3.3.8. The service provider will do the lifecycle management of the licenses including initiation of procurement request, after purchase, allocation, de-allocation, license renewal alert, license pool management.
3.3.9. Software Licenses Tracking & Management - This includes number of licenses for particular software, which NABARD has purchased, how many have been deployed, what is the entitlement etc.
3.3.10. Should support management of multiple licensing models based on User, Machine, IP, Core etc.
3.3.11. And any other related activities.

3.4. Patch Management using the tool

3.4.1. The ITSM service should include a patch management solution that offers all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating systems.
3.4.2. All critical application/software should also be patched as soon as patch/upgrade is available.
3.4.3. Assist, Develop, Manage and Monitor suitable Policies, Procedures and deployment strategy for Patch Management.
3.4.4. Maintain an up-to date plan for deploying and managing patch management.

3.4.5. Install and test patches and updates in Test environment provided by NABARD and after approval roll-out in the client computers

3.4.6. A practical and up-to date roll back plan has to be adopted in case of failures.

3.4.7. Raise Change Management for deployment of patches or updates.

3.4.8. Schedule shutdown of production system and inform users before applying patches, updates to Servers.

3.4.9. Implement patches as per approved deployment strategy.

3.4.10. Follow up and co-ordinate with OEM/ 3rd party support vendors for patch deployment on all devices.

3.4.11. Build a suitable backup and disaster recovery procedure for maintaining 100% availability of the Patch Management Server and resources.

3.4.12. Report on installed and missing patches

3.4.13. Removal of Software and service packs in case of need and roll back of patches and service packs in case of need.

3.4.14. Capability to identify the devices where patches are applied but not yet activated (pending restart).

3.4.15. A quarantine area has to be maintained for isolating the devices that are not patched up/updated with requisite updates.

3.4.16. Able to communicate effectively at all levels of the organization, and with Vendors in written and oral format.

3.4.17. Maintain smooth operation of multi-user computer systems, including coordination with network, software, and system engineers, PC desktop technicians, project managers, end users, and customer and IT management.

3.4.18. Interact, meet, discuss, and troubleshoot issues with Venodrs; evaluate Vendors products, services, and suggestions.

3.4.19. Maintain security audit information in tracker sheet for all patching related activities.

3.4.20. The tracker to be shared with DIT on weekly basis for review.

3.4.21. And carrying out other related activities

3.4.22. Solution should support system architectures.

3.5. Domain Services Management

The ITSM Service Provider should be capable of installation, configuration of solution along with other administrative tasks:

3.5.1. Existing Domain Server and User Admin have to be managed effectively with the help of suitable tools.

3.5.2. The service should include plan, design and set up and upgrade of additional controllers/forest during the contractual period.

3.5.3. Should co-ordinate, guide and assist in integrating any other systems for SSO /2FA and also digital certificate.

3.5.4. Root domain administration (AD & LDAP) by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.

3.5.5. Administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, and providing administrative support for print, file, and directory services.

3.5.6. Periodic reviews of domain level rights and privileges

3.5.7. Periodic AD (Active Directory) data updation and data interlinking with HRMS for auto updation.

3.5.8. AD integration with other applications

3.5.9. Any other related/similar activities.

3.6. File Services Management

A Windows File Server is being used in NABARD with specific usage space for departments and Regional offices. The same setup has to be managed by the ITSM Service Provider. The ITSM Service Provider should support this.

3.6.1. Functionalities of the File Server

A file server provides a central location for storing and sharing files across the network. ITSM Service Provider should be able to perform following roles:

a. Storage management: This console allows administrators to manage shared folders and allows users to access shared folders over the network.

b. Distributed File System (DFS): Provides tools and services for DFS Namespaces and Replication services.

c. DFS Namespaces: Allows user to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears as a single shared folder with a series of subfolders.

d. Replication: Allows to synchronize files/folders on multiple servers across the network.

e. File Search: Fast file search capabilities

f. Indexing service: Allows indexing of files and folders for faster searching.

g. The access to files should be based on User Rights controlled by Domain Services.

h. Selective Syncing of data in fileserver with cloud.

i. The ITSM Service Provider should be capable of installation, configuration, and management of the above stated file server.

j. Replication of the files/folders and capable of handling the File Services Management functionality.

3.7. Storage Management

The ITSM Service Provider should be familiar with setting up, configuration and usage of the prescribed storage management environment and is required to carry out the following activities:

3.7.1. Incident Management

Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.

- **a.** Configuration of SAN whenever a new application is hosted on the SDC. This shall Include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc
- **b.** Monitoring service availability, resource usage
- **c.** Troubleshooting system alerts with knowledge base
- **d.** Network reachability
- **e.** Administer SAN storage arrays and SAN fabrics and Participate in SAN on-call rotation
- **f.** Providing timely compliance to the audit observations related to storage infrastructure as observed during various internal/ external audits
- **g.** Preparation/Revision of Standard Operating Procedure (SOP) document for the Storage Administration.

3.7.2. Problem Management

- **a.** Closure of incidents effectively.
- **b.** Liaise with service providers for escalation and Root cause analysis
- **c.** Preparation of Preventive Maintenance calendar and configuring replication.
- **d.** SAN / NAS access control review.

3.7.3. Performance & Audit Management

- **a.** Monthly / Fortnightly incident analysis.
- **b.** Audit of administrator accounts.
- **c.** Preparation of capacity planning report.

3.8. Backup Management (All Servers at DC and DR)

- **a.** Performing backup operations for the servers as per the defined backup strategy.
- **b.** Ensuring proper storage and handling of media to prevent data loss.
- **c.** Conducting restoration drills with sample backed-up data on a quarterly basis to confirm data integrity.
- **d.** Maintaining log sheets of all backups taken at DC, DR and other locations.
- **e.** Implementing best practices on backup.
- **f.** Installation, re-installation, upgrade and patch deployment of the Arcserve, HPDP, etc. in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.
- **g.** Generation and publishing of backup reports periodically

h. Coordinate with the backup tape movement service provider/ courier agency and the identified nodal officer(s) for sending/ receiving tapes. Maintain tape movement logbook at DC & DR.

i. Coordination for maintaining inventory of off-site tapes at respective locations i.e., DC, DR, Head Office etc.

j. Tape/ LTO library management – loading and unloading tapes, etc at DC & DR.

k. Forecasting tape requirements and giving timely indent to concerned team for timely procurement of the new tapes/storage

l. Reporting of failed backups with critical alerts and ensuring that those are restarted and completed successfully within the backup cycle

m. Update/ Maintain Standard Operating Procedure (SOP) documents

n. Regular review of backup process and assist team to manage capacity planning.

o. Weekly movement of tapes between DC and Head Office, Mumbai, Delhi RO and DR site (Preferably on Friday)

p. Insertion of tapes in tape library at DC & DR site

q. Ejection of tapes from tape library at DC & DR site.

3.8. Data Center and Server Management

3.8.1. ITSM Service Provider should be capable of installation, configuration, and usage of the prescribed tool. Additionally, key points of expectations from the personnel are:

a. Regularly monitor and log the state of environmental conditions and power conditions in the Datacenter.

b. Service support at DR is required as and when required.

c. Periodic review arrangements at Data Center(DC&DR) in terms of cooling, power, positioning of racks &other hardware etc. on an annual basis. The SP shall be required to do first such assessment and submit a report thereon within a period of 2 months from the date signing of contract.

d. Coordinate with NABARD and third-party Service Providers to resolve any problems and issues related to the Datacenter & DR Site environment conditions. Power, air-conditioning, UPS, LAN, Servers, racks, fire, water seepage, dust cleanliness, implementing any changes, layout of infrastructure within the Datacenter & DR Site etc.

e. Suggest/Assist NABARD on best practices of the industry which may be required to be implemented in Data Center.

f. Patch management, upgrades to the systems.\

g. Ensure compliance of NABARD IT Security policies and compliance pertaining to Physical Security equipment in the DC.

h. Maintain high server availability through active performance monitoring and low impact, on- demand remote management services for devices present at DC&DR.

i. Installation, Updation configuring, hardening, trouble shooting of system (Hardware, Firmware and software) across all locations of NABARD

j. Mounting and Unmounting of all hardware components and Cabling, labling, tagging.

k. In case of repetitive hardware failure (three times in a period of three months) during warranty and AMC period, ITSM should coordinate to ensure that they are replaced by equivalent new equipment by OEM/Vendor as per SLA between NABARD and OEM/vendor.

l. Capacity planning and life cycle management of servers and other hardware and IT systems.

m. Online tracking and Inventory management of all the hardware devices including spare materials and periodical updation and review of the same

n. Regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.

o. All firewall, critical servers logs to be maintained for a period defined by NABARD.

p. Management of load balancers

3.8.2. Manage Nutanix Virtualized environment and other HCI virtualized environment including ODA and other cloud. The Nutanix (Virtualization) and other HCI equivalent skill set requirements are as below:

a. Knowledge and administration of industry leading virtualization software / technologies.

b. Knowledge of Nutanix virtualization, VM replication, FLOW, LEAP, XPLAY, prism central, etc.

c. Design and develop service virtualization framework.

d. Configure, deploy, monitor and support Nutanix nodes and clusters.

e. Define best practices, processes for service virtualization.

f. Maintain and configure Service Virtualization tool.

g. Troubleshoot the issues.

h. System installation and maintenance of Windows, AIX and Linux systems.

i. Windows, Linux, AIX, Arcserve, HPDP and Nutanix administration.

j. Knowledge of data center operations.

k. Administration of DNS (IPAM), SMTP, FTP, SSH, LDAP, and NFS services.

l. Patch management, upgrades to critical systems.

m. SAN/NAS storage systems knowledge.

n. Hardware, software and network troubleshooting.

o. Understanding of new business initiatives and the implementation of technologies to facilitate them.

p. Manage systems to achieve 24x7 availability.

q. Work closely with the storage, network and development groups to ensure business continuity.

r. Conduct trainings, mentor and coach teams on Service Virtualization

s. Valid Nutanix NCP-MCI-5 certification or higher.

t. Administering/monitoring Nutanix PRISM Console along with Nutanix nodes, clusters, hosted VMs in DC and DR. Further, the SP shall also monitor, upgrade and update Acropolis OS, AHV Hypervisor etc. Work will involve regular creation of VMs, cloning and monitoring performance of each VM. This shall require conducting regular health checkups and submit regular reports on overprovisioned VMs in terms of RAM, memory, cores etc. for the VM and cluster. Perform capacity planning from time to time.

u. Co-ordinating with necessary stakeholders (after due approvals from authority) for allocating appropriate resources and providing technical inputs for best practices wherever necessary for VM creation, cloning and monitoring performance of each VM

v. Regular co-ordination and advisories related to the conduct of DR Drill which take place every quarter.

w. To act as a trusted advisor to customer IT Teams, providing guidance as well as suggesting Nutanix and other VMware best practices.

3.8.3. JBoss Administration:

a. Support for CLMAS Upgrade for NABARD and its subsidiaries and RADP Platform

b. JBoss Installation and JDK configuration

c. JBoss Hardening and Upgrade

d. .ear, .jar, .war file Deployment

e. .jsp file attachment in tmp folder

f. App to Database connectivity configuration

g. Java Heap size changes

h. Port configuration (8080,18080, http and https)

i. Process kill JBoss

j. JBoss Service start / stop

k. Logs monitoring

l. New instance creation

m. Configuration file changes

n. SSL certificate installation

o. Daily Health checkup of JBoss Application Server

3.9. Network Management Services

ITSM Service Provider should be familiar with all the functionalities of Network Management Services and should broadly carry out the following responsibilities:

3.9.1. Monitoring:

a. Bandwidth utilization, end user bandwidth.

b. QoS and traffic shaping requirements/SDWAN management

c. Link latency
d. Uptime of all devices and servers.
e. Port utilization and growth
f. Marry port and patch panel utilization for audits
g. Audit and advice on rack utilization and growth
h. Inform the County of growth requirements for cabling such as network drops or fiber backbone Monitoring of Traffic Pattern over WAN
i. Follow up with Regional Offices for connectivity related issues
j. Monitoring and troubleshooting of L2 /L3 switches.
k. Monitoring Jitter, Latency, Availability, Bandwidth usage
l. Managing existing Firewalls, UTM, and VPN Services.
m. SDWAN monitoring, management and troubleshooting.
n. Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.
o. Managing NAC setup.
p. Managing Wi-Fi setup.
q. SFMS support

3.9.2. Vendor Management:

a. Enforcing SLAs with external networking Vendors.
b. Opening and managing support cases with external networking vendors/ISPs for various issues such as offline connections and SLA violations
c. Maintaining escalation matrix and ensuring the creation escalation matrix wherever required.
d. BGP etc and other NOC related coordination with ISP
e. OEM/SI related coordination for hardware issues.
f. Coordinate with these vendors for support services.
g. Maintain good relations with them on behalf of NABARD.
h. Logging calls, coordination and follow-up with vendors.
i. Escalation of calls to the higher levels at vendor's side in case of requirement.
j. AMC/ Warranty/ Support Tracking
k. Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the vendor will be made separately by NABARD)
l. Management of assets sent for repair.
m. Maintain database of the various vendors with details like contact person. Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with vendors, Coordinate and follow up with the vendors and ensure that necessary spares exchanged.
n. Analyze the performance of the vendors periodically (Quarterly basis or as specified).

o. Keep NABARD updated on the services and performance of these third-party vendors.

p. When a new solution software is introduced, training to users to absorb and leverages the technology for business should be invariably arranged. And other related activities.

3.9.3. Administration:

a. Managing routers, switches, firewalls, load balancers, wireless access points, and any other networking equipment

b. Assigning, allocating, and auditing network ports

c. Assigning and reassigning VLANs

d. Administering QoS policies as needed

e. Administering 802.1X authentication configurations where applicable

f. Firmware, application, controller, and operating system patching and maintenance

g. Maintain, audit, and extend the given IP schema and routing architecture

h. IPv4 with the intention to include IPv6 in the future

i. Maintain, audit, and extend multicast support throughout the network where applicable

j. Any other work assigned from time to time.

k. IS audit related information should be provided by the ITSM Service Provider.

l. Providing GUI based interfaces to readily check MPLS links status and utilization, health status of devices, Application based traffic (QOS) across all the locations ROs/HO

3.9.4. Lifecycle Management:

a. Inform the bank of bandwidth requirement/infrastructure upgrade and upgradation on a quarterly basis.

b. Participate in the identification and purchase of additional or replacement equipment

3.9.5. New Project inclusion:

In case bank is in process of implementing a new project. The requisite change request for successful implementation, management and operational support of the project should be submitted by ITSM Service Provider on request

3.9.6. FMS services for Network at HO/DC

ITSM Service Provider should be familiar with all the above-mentioned functionalities of Network Management Services and should broadly carry out the following responsibilities:

3.9.6.1. Monitoring

a. Monitoring of the main/backup Links and reporting\
b. Monitoring of Bandwidth utilization, latency, packet loss etc.
c. Managing NAC setup.
d. Managing Wi-Fi setup.
e. Monitoring of Traffic Pattern over WAF
f. Follow up with Regional Offices for connectivity related issues
g. Monitoring and troubleshooting of L2 /L3 switches.
h. Monitoring Jitter, Latency, Availability, Bandwidth usage
i. Managing existing Firewalls, UTM, and VPN Services.
j. SDWAN monitoring, management and troubleshooting.
k. Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.

3.9.6.2. Incident Management

a. Call logging and co-ordination with MPLS VPN service provider for restoration of link
b. Co-ordination with MPLS VPN service provider for ensuring backup Inks are made operational in the event of failure of primary and secondary links
c. Follow up with Service Provider to get detailed RFOs/RCA.
d. Prepare the Link wise outages and calculate the SLA Report to enable processing of the Service Provider Invoices
e. Prepare the Detailed payment note for due processing depending on SLAs.

3.9.6.3. Configuration Management

a. Configuration of L2 switches for administration and L3 Switches for VLAN creation / hardening etc.
b. Installation & Upgrade of switches as and when provided by the OEM/SI.
c. Changing configuration based on NABARD requirement and follow-up with MPLS VPN service provider for application of same on all routers.
d. Maintaining / Updating the WAN diagram at all locations/offices in co-ordination with NABARD IT team and Local Service Provider
e. Maintaining complete inventory of network hardware along with interfaces. IP address, Device OS version etc.

3.9.6.4. Reporting

a. Maintenance of daily/Weekly and monthly uptime report.
b. Present monthly performance review report with highlights/lowlights etc.

c. Collection of daily / weekly and monthly uptime/downtime report from MPLS VPN service provider.
d. Verification of daily report with the fault ticket generated by the MPLS VPN Service provider.
e. Cross verification of daily report with weekly and monthly report and calculation of uptime / downtime.
f. Co-ordination with MPLS Service provider for the replacement/up keep
g. Maintenance of defective Networking Hardware/Software (Like Routers. Modems. Switches etc.) and escalation, if necessary.

3.9.6.5. Advisory Services

a. Advisory services for revamping networks and introducing new network devices and services are also needed.
b. Periodic review mechanism should also be introduced for service improvements in this work area.

3.9.6.6. Onsite Support Engineer's Role for Network Animator tool (But not limited to this),

a. The engineer will perform following L1/L2 tasks in NMS solution with regards to the tools implemented at bank.
b. Perform daily tools health check based on checklist (services, processes, log file for any errors, application disk.
c. Perform all L1 level troubleshooting (Tool Management System Level) and assist Bank's Network Support team for troubleshooting.
d. Perform MACD (Move/Add/Change/Delete) activity such as adding/removing N/W devices, Servers from,
e. Perform Tasks like adding/modifying assignment group members, categories.,
f. Perform L1 level troubleshooting and follow L2 escalation matrix for non-resolved incidents.,
g. Coordinating for for L2 troubleshooting.,
h. Act as coordinator and provide assistance to OEM's remote support teams for troubleshooting/resolving the product,
i. Ensure all Service Requests, Incident and changes are logged and tracked till closure.,
j. Generating out of box reports as and when required by Bank.
k. Analyze network bandwidth report and device utilization to advice NOC team for Bandwidth up-gradation etc.
l. Daily MIS reporting of all the critical links.
m. Log the call with the OEM for critical tools issues,

3.9.6.7. Onsite Support Engineer's Role for NCCM tool (But not limited to this)

- **a.** Any configuration changes requested by bank forDC/DR or branch devices.
- **b.** Take care of configuration change and roll back as per bank person request.,
- **c.** Do the solution fail over testing on critical devices b/w NLS and DR on weekly basis.,
- **d.** Take back up for all network and security devices on daily basis.,
- **e.** Creating any new configuration/ configuration template/job/tasks etc as and,
- **f.** DC/DR/Branch devices hardening configuration changes as per banks network,
- **g.** Syncing of DC& DR devices on weekly basis.,
- **h.** Monitor the solution intimate banks on any compliance breach & rectify based on bank team request as and when required.,
- **i.** Share compliance report on daily basis.,
- **j.** Inform banks team in case of any alert /error observed in any device configuration and act according to,
- **k.** Failover testing of critical devices on weekly basis as per bank team's request.,
- **l.** Ensure that all backups are happening correctly and need to maintain and submit the checklist on,
- **m.** Prepare and submit day to day activity report on daily basis.,
- **n.** Periodic discovery of all all the network devices & share the list of noncompliance devices and do the required changes to make it compliant only after bank's team permission.,

3.9.7. SDWAN Forcepoint SMC

- **a.** Management of the architecture –documentation of present architecture, BGP peering management with ISP.
- **b.** IP Sec tunneling for various sites and traffic management on the tunnels
- **c.** Routing on various devices at ROs/HO
- **d.** QOS as per Banks requirement
- **e.** Configuration of Any other feature available on SDWAN as required by bank

3.9.8. Wifi controller

- **a.** Definition of levels according to network security
- **b.** Management of Guest access
- **c.** Management of access privileges.

3.9.9. Support services for CCIL, RTGS/NEFT applications and payment infrastructure management:

- **a.** Onsite support for issue-resolution on all working days and as per emergency requirement beyond working days and holidays.

b. Remote support Telephonic / Network
c. Preventive Maintenance and System Health Checks
d. D.R. Drill assistance
e. Upgrade / Version Management
f. Re-installation / Re-location of Systems and Applications
g. License Management (Track and coordinate for validity)
h. CCIL Systems Help Desk Support
i. Single point of contact for
  i. Regulatory Authorities (RBI, IDRBT, CCIL)
  ii. Applications vendor
  iii. Principals (IBM, Microsoft, Cisco etc.)
j. Service Window
k. Trouble shooting and issues management
l. Patch Management (OS and Middleware)
m. Performance Management
n. Configuration of MQ7 on servers.
o. Trouble shooting and issues management
p. Escalation of issues to appropriate vendor
q. Testing of client server connectivity, member to host connectivity and application level testing.
r. Network Monitoring
s. Support for obtaining digital certificates and configuration of same with all related applications.

3.9.10. Wi-FI Solution at DC/DR, HO and RO

a. Management of the architecture –documentation of present architecture, peering management with ISP, access controls, user segmentation, policy and firewall management
b. Operation administration and Maintenance of the solution at all the locations.
c. Security and network management.
d. Routing on various devices at Ros
e. Coordination with all the relevant stakeholders.
f. End to end life cycle management.

3.10. IT Security Management

IT security management is a vast area involving logs at various devices including, firewalls and other security devices, password management, change management, etc. Hence, the required functionalities have been grouped under several categories as follows:

3.10.1. IT Compliance and Log Management

A suitable Syslog Server has to be incorporated with the following capabilities:

- **a.** Collects logs from heterogeneous sources.
- **b.** Decipher any log data regardless of source and log format
- **c.** Rule-based event correlation for proactive threat management
- **d.** Pinpoints breach attempts, insider threats, policy violations, and more, without any manual intervention
- **e.** Generate pre-defined compliance reports for event logs and syslogs to meet various standard compliances like PCI DSS and etc.
- **f.** Facilitate to create custom reports for new compliance to help comply with growing new regulatory acts demanding compliance in future.
- **g.** Generate an alert in case of failure of log collection in regard with any log sources.

3.10.1.1. Incident Management Services

- **a.** Perform continuous Monitoring on WAF and Web Proxy Consoles.
- **b.** Prevention duties include system monitoring, assessment, testing, and analysis designed to identify and correct potential security breaches.
- **c.** Protect and improve organizational security by preventing, averting, and mitigating security threats.
- **d.** Perform following steps: Incident logging, Incident categorization, Incident prioritization., Incident assignment., Task creation and management., SLA management and escalation., Incident resolution.
- **e.** Have collaboration with ITSM Security Team, ITSM Patch ITSM ITSM Service Provider and ITSM Network team to perform incident Analysis.
- **f.** Analyze daily reports (AV reports network devices reports, IPS, etc.).
- **g.** Creation and Maintaining of Tracker for incidents.
- **h.** Perform RCA for Cyber security incidents (email phishing, Antivirus infections, repeated logout, etc.).
- **i.** Preparing documentation for each incident analyzed.
- **j.** Providing support for application-level settings at WAF.
- **k.** Providing support for blocking /allowing any website at web proxy solution. Need to raise a ticket/case with OEM to resolve the website issue if any.
- **l.** Miscellaneous Activities to be taken up by ITSM Service Provider

3.10.1.2. Firewall Security and Configuration Management

- **a.** Centrally collect, analyze and archive logs from all security devices
- **b.** Maintain firewall/UTM/SDWAN logbook for all devices location wise separately.

- **c.** Automate compliance audits with reports for regulatory mandates such as PCI-DSS, ISO 27001, etc.
- **d.** Perform firewall rule base review and device configuration analysis and Generate reports on quarterly basis.
- **e.** Get real time alert on 'who' made 'what' changes, 'when' and 'why' to firewall configuration
- **f.** Change management reports to get a complete trail of all the changes done to firewall configuration
- **g.** Monitoring Internet usage (overuse and misuse) of employees
- **h.** Monitoring outgoing traffic through the proxy, obtain details on user generating traffic, website access and bandwidth consumed
- **i.** Real-time notification when a user tries to access restricted sites
- **j.** Network traffic monitoring to get instant notifications upon sudden spike in bandwidth
- **k.** Analysis of user or network activity consuming high bandwidth with interface-wise bandwidth usage reports
- **l.** Getting detailed information on all possible network attacks and security breaches in organization's network
- **l.** Knowing which viruses, malware, BOTs, APT, etc are active on the network, the hosts that are affected and more; Searching logs and report generation based on search results
- **m.** Identifying highly used firewall rules which can be optimized to enhance network security
- **n.** Identifying unused rules and/or modifying/removing them to improve firewall performance (to comply with all IS policy requirements of GoI/CISO)
- **o.** All important GoI and Industry websites needs to be monitored regularly for various policy updates and with suitable approval from IT team of the Bank. All necessary and suitable policies should be applied by the ITSM Service Provider
- **p.** Security Information and Event Management (SIEM)
- **q.** The monitoring of endpoints, vulnerability information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS) and detection (IDS) systems

3.10.1.3. Privileged Password Management

- **a.** Storage and organization of all privileged identities in a centralized vault
- **b.** Secure sharing of administrative passwords with the members of the team on need basis
- **c.** Self-resetting of passwords
- **d.** Controlling access to IT resources based on roles and job responsibilities
- **e.** Auditing of all privileged accesses and complete recording of all actions

3.10.1.4. Network Behaviour Anomaly Detection

- **a.** Monitoring network security in real time

b. Monitoring internal and external threats
c. Classifying threats into various categories (e.g., DDoS, Scan/probe, Suspect, etc)
d. Carrying out detailed forensic investigation
e. Sending alert notification via Email or SMS

3.10.2. Active Directory Management and Reporting

a. Automatic routine AD management and reporting activities for AD administrators
b. Facilitates creation, management, and deletion of AD objects in bulk.

3.10.3. Self-Service Password Management

a. Allow users to reset/change their passwords and unlock their AD accounts, without IT intervention through web based portal using SMS and authenticator
b. Remind users automatically about soon-to-expire passwords by email and SMS
c. Allow users to update their profile details, like contact details in Active Directory through web based portal.

3.10.4. Network Configuration Management

a. Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI
b. Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes
c. Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.
d. Automating all repetitive, time-consuming configuration management tasks. Applying configuration changes in bulk to multiple devices.
e. Recording sessions: Getting complete record of who, what and when of configuration changes. Recording actions, archiving.

3.10.5. Active Directory Backup and Recovery

a. Automated incremental backup of Active Directory Objects
b. Change tracking to undo changes
c. Detailed version management to each attribute change
d. Provision to roll back Active Directory to an earlier state

3.10.6. Required ITSM Services

The ITSM Service team should be capable of performing the above stated activities using the prescribed tool(s). Some more key activities are:

a. Monitoring Status of security components and alerts, ports on firewalls
b. Monitoring Bounced Messages
c. Spam database update status
d. Monitoring Service Status (Up & Running),
e. Virus Alerts from Critical Servers
f. Logging security incidents
g. Assigning severity to the Incidents logged based on the definition.
h. First level analysis (investigating problems) and closure of known and low priority security incidents. Logging Problem Ticket for unresolved Incidents
i. Sending Security Alert messages on newly found vulnerabilities
j. Monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
k. Maintenance of an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, solution servers, web servers, databases, security solutions, messaging solutions, etc.
l. Implementation of Change and Release Management
m. Installation of security patches & bug fixes
n. System health checks for all security devices
o. Vulnerability scanning
p. Adhering and Implementing guidelines and policies (BS7799)
q. Defining Rules in line with the security policy.
r. Responding to events and fixing vulnerabilities in IT infrastructure (like IPS, Checkpoint logs)
s. Implementation of Firewall exclusions
t. Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.
u. Respond to security breaches or other security incidents and coordinate with respective OEM in case a new threat is observed to ensure that workaround / patch is made available for the same.
v. Maintenance and management of security devices including but not limited to maintaining Firewall services to restrict network protocols and traffic detecting intrusions or unauthorized access to networks, systems, services, applications, solutions or data protecting email gateways, Firewalls, servers from viruses.
w. Periodic reviews of domain level rights and privileges
x. Modifying access permissions and adding new access permissions of security policies on existing firewall.
y. Up-gradation of the firewall and IPS devices.
z. Signature update for IPS device.
aa. Configuration backups for all security devices

bb. Syslog server configuration & management including review of logs.
cc. Managing / monitoring the IDS/IPS tool and policies as per guidelines of NABARD.
dd. Modifying the policy for IDS/IPS/Firewall based on observed trends / security lapses.
ee. Changing network address translation rules of existing security policies on the firewall.
ff. Adding new network address translation rules on security policies on existing firewall.
gg. Diagnosis and troubleshooting of the problem faced on firewall and faced by the IDS/IPS.
hh. Managing / monitoring the IDS/IPS tool and policies
ii. Periodic / Critical reporting to NABARD officials based on Firewall / IDS / IPS activities
jj. Managing configuration and security of Demilitarized Zone (DMZ)
kk. Alert / advise NABARD about any possible attack / hacking of services, unauthorized access / attempt by Mental or external persons etc.
ll. Resolution and restoration of services in case of any possible attack and necessary disaster management
mm. Shutdown of critical services to prevent attack (internal or external)
nn. Advise to improving network/Data Center security to protect NABARD's data / information from both internal and external persons/attack.
oo. Resolution and restoration of services in case of any possible attack and necessary disaster management.
pp. Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.
qq. And other related essential activities to ensure that the functionalities of IT Security.

3.10.7. Checkpoint/Fortinet/Forcepoint/SDWAN Security Requirements

3.10.7.1. The Security Engineer should be skilled to carry out the following areas and should be a Certified Security Administrator.

a. Install the security gateway in a distributed environment
b. Configure rules on Web and gateway servers
c. Create a basic rule base in Smart Dashboard and assign permissions
d. Schedule backups and seamless upgrades with minimal downtime
e. Monitor and troubleshoot IPS and common network traffic

3.10.7.2. The Security ITSM Engineer should be capable of the following:

a. Be prepared to defend against network threats
b. Evaluate existing security policies and optimize the rule base
c. Manage user access to corporate LANs
d. Monitor suspicious network activities and analyze attacks
e. Troubleshoot network connections
f. Protect email and messaging content

3.11. Data Base Administration

3.11.1. Database monitoring

a. Creating user-specific SQL or PL/SQL metrics with warning notification
b. Execution of user-specific scripts on Windows platform
c. Creating customized SQL reports with email notification
d. Dynamic visual indication of problems in the console

3.11.2. Instance access to the following information

a. Size of databases
b. Free space in table spaces
c. User table spaces, spaces occupied by objects
d. Object/system privileges of users/roles, reasons of granting
e. List of roles/privileges granted according to a certain document
f. Description of users, their passwords, reasons for creation
g. List of scripts in a specific database and their purpose
h. Technical documentation of any database
i. Log of actions/crashes/incidents in any database
j. And other related areas.

3.11.3. Log of database changes

a. Date of creation/deletion of users/roles, log of privilege changes
b. Time of granting/revoking privileges, reasons for granting
c. Table space sizes
d. Time and date of database objects creation and deletion
e. History of database operations performed in the system (e.g., granting of privileges, creation of table spaces, etc.)
f. Connections to the database, with names of computers and solutions
g. And other related areas.

3.11.4. Automation of routine operations

a. Moving of tables. Automatic detection of available table spaces for moving
b. Automatic rebuilding of indexes invalidated during the moving of tables of their partitions
c. Quick creation of table spaces, automatic naming
d. Adding and resizing files, automatic naming
e. (v) Splitting, exchange and removal of table partitions. Support of partitioning by various criteria (dates, interval).

f. and revocation of system or object privileges using lists
g. User creation and editing
h. Top queries by CPU
i. Top Queries by IO
j. Top CLR Queries and Waits
k. Top Slow Running Queries
l. Frequently Executed Queries
m. Most Blocked Queries
n. And other related areas.

3.11.5. Storage of documents and descriptions

a. Storage of database descriptions, their versions, paths, etc.
b. Descriptions of users and their passwords stored in an encrypted form
c. Comments to the privilege being granted (including the preferred revoking date to be monitored)
d. Comments to database files, table spaces, warnings
e. Action, crash or incident logs for each database
f. Descriptions of SQL and OS scripts, their relation to bases and hosts
g. Technical and work documentation on any database
h. And many more.

3.11.6. Required Services

The Data Base Administration (DBA) should be familiar with following DBA activities. Some more important activities include:

a. The DBA services shall cover existing production, testing & development DB environments that are in the organization at all locations.
b. New DB implementation , migration support and services& Services for Microsoft SQL 2012, 2016, 2019 , Oracle 11g , 12c, 19c, Mysql 7,8 , Postgres, PGsql & higher versions. Support and operation for any forthcoming application databases other than listed above.
c. –Specific activities only need to be handled by ITSM team. Enterprise application owners will be taking care of applications. Primary ownership will be with application owners and primary work to be done by enterprise application owners.
d. Change management of database schema, storage, disk space, table space, user roles, backup and purging etc.
e. As per IT security policy of the organization, ensure database patch management with minimum downtime and recommend appropriate patches of Operating System relevant to database.
f. Managing database upgrades operations. Including minor and major upgrades of all existing and newly introduced applications in future.
g. And other similar activities.

h. Advisory services to enhance application performance and user experience, user role management.
i. Proactive cleaning of extra tables.
j. Provide automation support.
k. Integration with different platform and systems.
l. Audit activity to be done frequently to review database schema, storage, disk space, table space, user roles, backup and purging etc.

3.12. Vendor Management

ITSM Service Provider should be familiar with installation, configuration and usage of the prescribed vendor management tool and should carry out the following responsibilities:

3.14.1. Coordinate with vendors for support services.
3.14.2. Logging calls, tickets, coordination and follow-up with vendors
3.14.3. Escalation of calls to the higher levels at vendor side in case of requirement.
3.14.4. Vendor SLA tracking and monitoring with alerts and escalations (including WAN Vendor)
3.14.5. AMC/ Warranty/ Support Tracking
3.14.6. Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the vendor will be made separately by NABARD)
3.14.7. Management of assets sent for repair.
3.14.8. Maintain database of the various vendors with details like contact person. Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with vendor Coordinate and follow up with the vendor and ensure that necessary spares exchanged.
3.14.9. Analyze the performance of the vendor periodically (Quarterly basis or as specified).
3.14.10. When a new solution (Hardware/software) is introduced, training to engineer/users to absorb and leverages the technology for business should be invariably arranged. And other related activities.
3.14.11. End to end lifecycle management of new solution(Hardware/software)

3.13. Help/Service Desk Services Management

The related ITSM Service Provider should be capable of installation, configuration and using the above said help/service desk tool and carry out the following activities:

3.13.1. Helpdesk resource should log all ticket received through various channels e.g. phone, email, IVR, sms, chatbot, MS-teams etc.

3.13.2. The Help desk team should be able to post the response back to the concerned people.

3.13.3. Helpdesk should classify and assign the ticket in appropriate section of ITSM services and other NABARD internal applications

3.13.4. Helpdesk tool should include tickets of all ITSM as well as NABARD internal applications and assign them to respective application teams.

3.13.5. If needed, the concerns/service requests can be escalated to concerned IT team who will be able to look into it.

3.13.6. Generate status report of pending/closed concerns on a daily/weekly/monthly basis.

3.13.7. Helpdesk should ensure that all calls to IT helpdesk are logged at a central helpdesk. All calls logged will have to be monitored and assigned to respective team /engineer / analysts and tracked for proper closure within the specified SLA limits. Helpdesk would ensure that the calls should be updated with the diagnosis carried out to close the call.

3.13.8. The service provider shall ensure that any change in resident engineers and/or helpdesk personnel is conveyed to the concerned NABARD officials one month in advance. The ITSM Service Provider would provide resumes of proposed ITSM resources (engineers/helpdesk personal)to the concerned NABARD officials. Only approved resources would be permitted to replace the outgoing ones.

3.13.9. The helpdesk shall provide support for distribution of computer peripherals on demand and maintain inventory of the same.

3.13.10. And should carry out other similar activities.

3.14. Non-Delivery of Services / PENALTIES & SLAs

3.14.1. The selected ITSM Service Provider will have to provide satisfactory service to achieve the service levels as given in "Expected Service Delivery". The service level performance will be recorded/monitored daily and will be reviewed on quarterly basis and non-performance will result in penalty being imposed.

3.14.2. The tools provided for monitoring and managing these services should give a detailed report for calculating the support calls including the response time, resolution time, penalty cost applicable etc. This should facilitate both the Service Provider and the Bank to directly arrive at the penalty cost applicable under all these services.

3.14.3. The total non-performance charges for a quarter will be calculated and deducted from the quarterly bill of the selected ITSM Service Provider. Annual Contract value will be calculated on the basis of the opening quarterly inventory after adjusting the addition or deletion, if any, during the previous quarter.

3.14.4. Penalty charges would be applied for those services, which have not achieved the stipulated service levels based on the table mentioned in Expected Service Delivery. There will be maximum penalty charge of 10% per Quarter of the Quarterly Contract value.

3.14.5. The calculation of the same will be done on a Quarterly basis as under - At the end of every month, the ITSM Service Provider will submit the average response time and average resolution time report. Rs 500/- per hour subject to a maximum of Rs. 3000/ per day for critical equipment and Rs. 300/- per hour subject to a maximum of Rs. 1500/- per day for all other equipment. Within 5 working days the original equipment should be delivered back to us.

3.14.6. Table for all ITSM services rating will be formulated in discussion with NABARD.

3.14.7. Spare Parts

3.14.7.1. If the original asset is not returned in the stipulated 5 days, a penalty of Rs. 2000/- per day for critical equipment and Rs. 1000/- per day for other equipment would be levied.

3.14.7.2. In case of a genuine problem of non-availability of spare parts with the principal, a letter / email to that effect should be forwarded to NABARD by the ITSM Service Provider. NABARD at its discretion may decide to waive off the penalty in such exceptional situations.

3.14.8. Covering for Absence of ITSM Services

3.14.8.1. The backup engineer in the centers should be trained in the presence of the main engineer and if need be, the backup engineer could be asked to manage the infrastructure in the supervision of the main engineer, for a couple of days. This will lead to a seamless backup of the main engineer when he avails of short spells of leave. Service provider should ensure that same engineer is available in absence of main engineer

3.14.8.2. In case suitable replacement is not given for leave/resignation/reassignment of ITSM personnel, a penalty of Rs.1000/- per day per personnel towards absence will be imposed. In case the resident officials are absent / late and a uitable replacement is not provided, a penalty of Rs. 200/- per hour subject to a maximum of Rs 1000/- per day will be imposed.

3.14.9. Expected Service Delivery

Sr No	Particulars	Response	Resolution	Penalty
1.	Desktops of Critical (such as Dealers at H.O, Risk Team) Depts. And Senior Officials at H.O.	15 minutes	30 minutes or immediate standby to be provided	Rs. 500/- per working hour delay or Rs. 3000/- per day whichever is less.
2.	Other Equipment: Desktops, Applications, Printers, Scanners, etc. at H.O.	30 minutes	2 hours. (1 working day if parts are to be replaced)	Rs 300/- per working hour delay or Rs 1500/- per day whichever is less.
3.	Laptops	30 min.	2 working days if parts are to be replaced.	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
4.	Resolution of OS related problems	30 min	12 hours	Rs. 500 per working hour delay or Rs 3000/- per day whichever is less.
5.	Servers, Network and related equipment, and all other equipment under warranty	30 min	Follow up, Co-ordination & Escalation within 4 hours	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
6.	R.O. Desktops, Laptops - OS / Application issues	30 minutes	2 Hours	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
7.	R. O. Desktops, Laptops - hardware issues	30 min	2 hours for troubleshooting and logging call with OEM for replacement of part / warranty machine.	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
8.	R. O. MPLS related issue	30 min	2 hours for troubleshooting and	Rs 300 per working hour delay or Rs

			resolution / providing report on findings.	1500/- per day whichever is less.
9.	Issues with Tools provided by the ITSM Service Provider	30 min	Follow up, Co-ordination & Escalation within 4 hours	Rs 500 per working hour delay or Rs 3000/- per day whichever is less.

3.14.9.1. The response & resolution time will be calculated from the time of lodging the call. When formatting and loading of all the software is required, additional two hours will be allowed for resolution. For calculating downtime, calls logged after closing time will be treated as logged at the opening hour of the following working day. Resolution time includes making the systems available for work with O/S uploaded.

3.14.9.2. ITSM Service Provider has to make alternate arrangements for leave/resignation/reassignment of ITSM personnel and intimate the same to NABARD at least one month in advance. A penalty of Rs. 1000/- per day per personnel towards absence will be imposed, if suitable replacement is not given (with the qualification & experience)

3.14.9.3. Also, to service the most obsolete or discontinued model as well, the ITSM Service Provider shall be liable for any loss or damage to the scheduled equipment caused due to negligence of the ITSM Service Provider during the contract period.

3.14.10. DOWNTIME - CALCULATION METHODOLOGY

3.14.12.1. 'UPTIME' of the hardware and system software = (Reckoned Hours minus Downtime /Reckoned Hours X 100 for the maintenance year.

3.14.12.2. Reckoned Hours = Uptime commitment per day X No. of committed days per Year

3.14.12.3. Uptime Commitment per day = Hardware and System Software Maintenance Support Time per day

3.14.12.4. Down Time will be counted from the time of reporting the maintenance call by NABARD to the ITSM Service Provider till the resolution of the problem / operations of the hardware and system software.

3.14.12.5. No. of committed days per Year = the number of working days of the NABARD during the year.

3.14.11. NON-PERFORMANCE CHARGES:

3.14.11.1. The selected ITSM Service Provider will have to provide satisfactory service to achieve the service Levels as given in Expected Service Delivery table. The service level performance will be recorded/monitored daily and will be reviewed on quarterly basis and non-performance will result in penalty being imposed.

3.14.11.2. The total non-performance charges for a quarter will be calculated and deducted from the quarterly bill of the selected ITSM Service Provider. Annual Contract value will be calculated on the basis of the opening quarterly inventory after adjusting the addition or deletion, if any, during the previous quarter.

3.14.11.3. Penalty charges would be applied for those services, which have not achieved the stipulated service levels based on the table "Expected Service Delivery" as mentioned above. There will be maximum penalty charge of 10% per Quarter of the Quarterly Contract value.

3.14.11.4. At the end of every month, the ITSM Service Provider will submit the average response time and average resolution time report.

3.14.11.5. The calculation of the same will be done on a Quarterly basis as under:

Rs 500/- per hour subject to a maximum of Rs. 3000/ per day for critical equipment) and Rs. 300/- per hour subject to a maximum of Rs. 1500/- per day for all other equipment. Within 5 working days of the original equipment should be delivered back to us.

3.14.11.6. The ITSM Service Provider may keep all IT assets in buffer stock in ready to use condition. The ITSM Service Provider may provide machine from buffer stock within 30 minutes from user request. If the machine is not provided in stipulate time, a penalty of Rs. 300/- per hour and Rs. 1500/- per day would be levied.

3.14.11.7. In case of a genuine problem of non-availability of spare parts with the principal, a letter / email to that effect should be forwarded to NABARD by the Principal. NABARD at its discretion may decide to waive off the penalty in such exceptional situations.

3.14.11.8. Non-performance charges will not be applied for that equipment under ITSM Service Provider management provided the calls are logged within the response time to the respective ITSM Service Providers and followed up with proper escalation.

3.14.11.9. In case suitable replacement is not given for leave/resignation/reassignment of ITSM personnel, a penalty of Rs.1000.00 per day per personnel towards absence will be imposed.

3.14.11.10. In case the resident officials are absent / late and a suitable replacement is not provided, a penalty of Rs. 200/- per hour subject to a maximum of Rs 1000/-per day will be imposed.

3.14.11.11. ITSM service provider will incorporate all above mentioned rules and conditions in their tool and provide online access to DIT management. They will also provide monthly and quarterly penalty sheet.

3.15. Documentation

3.15.4.1. ITSM Service Provider will provide support for coordinating with other external vendors (such as ISPs etc. providing IT services to

NABARD) for resolution of the problems related to IT issues/projects. The Scope covers the IT vendors of NABARD at all locations.

3.15.4.2. Documentation & Reporting Deliverables:

a. Maintaining database of the all vendors

b. Contact person/Telephone / Fax / Email, etc

c. Escalation Matrix / Response time

d. Co-ordinate with vendors for email technical support & other technical problems.

e. Generate reports of calls logged, resolved, escalated and pending with time and date and monitor vendor performance using tools.

f. NABARD software/hardware configuration, network diagrams documentation.

3.15.3. Technical Documentation

3.15.3.1. Following documents should be delivered by the ITSM Service Provider to the Bank for every software including third party software before software/service become operational, which includes, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures etc.

3.15.3.2. The ITSM Service Provider should also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable. The ITSM Service Provider should also provide the MIS reports as per requirement of the Bank. Any level/version changes and/or clarification or corrections or modifications in the above-mentioned documentation should be supplied by the ITSM Service Provider to the Bank free of cost in timely manner.

3.15.4. Reports

ITSM Service Provider shall submit the reports on a regular basis in a mutually decided format. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients. ITSM Service Provider shall submit certain information as part of periodic review as and when required by the Bank

Following is the indicative list of reports:

3.15.4.1. Daily reports (to be submitted on next working day)

a. Log of backup and restoration undertaken.

b. Summary of issues / complaints logged at the Help Desk.

c. Summary of resolved, unresolved and escalated issues/complaints.

d. Summary of resolved, unresolved and escalated issues/complaints to OEMs/SP/NABARD support teams.

e. Mail traffic report - list of top users sending /receiving highest number of mails.

3.15.4.2. Weekly Reports (to be submitted on the first working day of the following week)

a. Issues/Complaints Analysis report for virus calls, call trend, call history etc. Summary of systems rebooted.

b. Summary of issues /complaints logged with the OEMs.

c. Summary of changes undertaken in the Data Center including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset etc.

3.15.4.3. Monthly Reports (to be submitted by 10th of the following month)

a. Component wise physical as well as IT infrastructure availability and resource utilization.

b. Summary of component wise Data Center uptime.

c. Summary of changes in the Data Center.

d. Log of preventive / scheduled maintenance undertaken. Configuration Management summary report.

e. Change Management summary report.

f. Release Management summary report.

g. Service Level Management - priority/severity wise response and resolution.

h. Service Failure Analysis, listing out escalations and downtime/outages, if any.

3.15.4.4. Account Dash Board, listing out:

a. Planned activities carried out during the month.

b. Unplanned activities carried out during the month.

c. Activities planned but missed specifying the reasons.

d. Challenges faced during the month.

3.15.4.5. Service Operations, listing out:

a. Service Desk Management - Location wise call summary for all on-site ITSM locations for last three months.

b. Helpdesk Management, listing out priority/severity wise calls logged with comparison for past three months.

c. Incident Management, giving category wise call details for critical overhaul areas with comparison for past three months.

3.15.4.5. Operational Activities

a. Location wise weekly visits done for off-site ITSM and attendance of the on - site resource personnel.

b. Service wise performance of activities as per scope of individual service areas.

3.15.4.6. Service Improvement Plan, listing out:

a. Concerns/Escalations with action plan.

b. Planned activities/initiatives.

c. Improvements planned, if any.

3.15.4.7. Incident reporting (to be submitted within 48 hours of the incident)

a. Detection of security vulnerability with the available solutions / workarounds for fixing.

b. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. - with root cause analysis and the plan to fix the problems

c. Software license violations.

3.15.5. The ITSM personnel are required to provide various documents/reports to NABARD on a time-to-time basis. Few important of them are highlighted here. the detailed Scope of Work may mention about many other such requirements.

S. No.	Service Components	Documents/Reports to be shared by ITSM personnel with NABARD (along with Frequency)
1.	AMC for Computers and Peripherals	Onsite maintenance service reports (daily)
2.	Inventory Management	i. List of hardware's (always updated - to be shared whenever required) ii. List of software's (always updated - to be shared whenever required) iii. List of licenses along with expiry dates, how many deployed, etc. (always updated - to be shared whenever required) iv. Configuration change report (whenever configuration changes)
3.	Patch Management	i. List of installed and missing patches (always updated - to be shared whenever required) ii. List of devices where patches have been applied but not yet activated (always updated - to be shared whenever required)

4.	Domain Services Management	i. List of all users, associated computers, and access permissions (always updated - to be shared whenever required) ii. Change requests (whenever it arises) iii. Audit report of administrative privileges (weekly)
5.	Storage Management	i. Storage server availability report (daily) ii. Network reachability report (daily) iii. Log of backups taken (weekly) iv. Capacity Planning Report (monthly)
6.	Data Center and Server Management	i. State of environment and power conditions (daily) ii. Assessment of data center in terms of cooling, power, positioning of racks, and other health parameters (first report after 2 months, and subsequently once in a year) iii. On-site inventory of critical equipment for the data center (always updated - to be shared whenever required) iv. Log register of visitors in data center (daily) v. Server availability report (daily) vi. Audit of server logs (weekly)

7.	Network Management	i. Inventory of network hardware (always updated - to be shared whenever required) ii. Logs of switches/routers (weekly) iii. Status of the switches/routers (daily) iv. Status of the links (daily) v. Traffic patterns (weekly) vi. Analysis of which user is consuming more bandwidth within the network (daily) vii. Report of network configuration changes (whenever such change occurs) viii. Periodic reports involving the following: • Alerts (real-time) • Outstanding tickets (customized) • Hourly Ticket Analysis (different time buckets - customised) • Incident Count • Docket Count with ISP - SP-wise and total • Problematic Links Details. • Device configuration changes - CRF confirmation • Average uptime per link in hours - monthly / percentage • RFO Analysis - Resolution Analysis ✓ Top 10 Inbound Utilization ✓ Top 10 outbound Utilization ✓ Top 10 Memory Utilization ✓ Top 10 CPU Utilization ✓ Uptime analysis of the Links ✓ SLA Compliance Report ✓ Capacity Planning Report ✓ Issues & Concerns
8.	IT Security Management	i. Logs of firewalls/IDS/IPS (daily) ii. Rules of firewalls/IDP/IPS (always updated -to be shared whenever required) iii. Report of change in security rules in firewalls/IDS/IPS (whenever such change occurs) iv. Report of security threats with proper identification of the nature (whenever it arises) v. Vulnerability scan reports (quarterly)

		vi. Pre-defined compliance report to meet standard compliances (like PCI DSS, ISO 27001 etc.) (whenever required) vii. Real time notification whenever an user tries to access restricted sites (whenever such case arises) viii. Real time reporting of active malwares in the network and its mitigation (daily) ix. Statistics of usage of firewall rules (may be required to optimize the rules) (quarterly) x. Miscellaneous Reports • IPS Report- Daily • Firewall Health status - Daily • Events Report - Daily • Summary of Changes - Daily • The above reports may be consolidated on weekly / monthly / quarterly basis
9.	DBA (Oracle, MySQL and MSSQL)	i. Report Change of data base users (whenever such thing happens) ii. Change of database schemas (whenever such thing happens)
10.	ITSM Service Provider Management	i. Log of calls to third party ITSM Service Providers, reasons, measures taken by the 3rd party ITSM Service Providers etc. (daily) ii. Report about performance of each 3rd party ITSM Service Provider (quarterly)
11.	Helpdesk and Service desk Management	i. Status report of raised/pending/closed concerns by the users (daily) ii. Report about concern escalations, their status (daily) iii. List of service ITSM service engineers along iv. with their resume (always updated - to be shared whenever required) v. Notification about change in service engineers (in advance) vi. Gate pass issued to visitors (daily) vii. Inventory of computer stationery and consumables (weekly)

3.16. Advisory Services

NABARD also will like to have advisory services by competent personnel of the ITSM Service Provider as part of ITSM Services. The ITSM Service Provider shall arrange for presenting a summary of the IT Services provided to the Bank vis a vis the best practices in the industry and shall make efforts to ensure that they are assimilated in the Bank.

Service Components	Documents/Reports to be shared by ITSM personnel with NABARD (along with Frequency)
Storage Management	(i) Effective storage management (ii) Capacity planning (iii) Suggesting best practices about back up
Data Center and Server Management	(i) Best industry practices (ii) Capacity planning
Network Management	(i) Advisories for revamping networks (ii) Periodic review for service improvement (iii) Best Industry Practices
IT Security Management	(i) Advisory for firewall/IDS/IPS rules (ii) Potential/emerging threats and preventive measures (iii) Best Industry Practices

3.17. Resource

Staffing/ Skill-Set / Qualification / Experience /Knowledge Sharing

3.17.1. HO onsite engineers - as per Bank's understanding a total of 25 engineers with necessary skillsets as indicated the Appendix III. However, the ITSM Service Provider is expected to propose a suitable team structure, composition and number of engineers after doing a complete study of the RFP document.

3.17.2. At all other 35 ROs & TEs locations, full time onsite engineers has to be placed as per details mentioned in Appendix III. He/she will be responsible for delivery, Management of all above said service components.

3.17.3. The key parameters for evaluating the team members would be:

a. Qualification & Certification
b. Total experience
c. Number of similar analytics assignments handled
d. Number of similar project duration assignments handled

The number of service engineers indicated in the table below is prescriptive only. The total number engineers needed for providing all the services sought at various locations (on-site and off-site) should be worked out so as to maintain the SLA standards and accordingly the solution should be built and provided.

The detailed break-up of project team members, their summarized job description and evaluation criteria are tabled below:

Sr. No.	Staff Profile	Job Description	Skill - set / Qualification /

			Experience /Knowledge sharing /Qualification & experience
1	Team Lead	Responsible for overall performance and delivery of the ITSM Services.	MCA /B. Tech / BE
		Should be Pro-Active	Mandatory certification: ITIL certified
		Should efficiently document and share with team and NABARD	Minimum 8 years of relevant experience as a IT Team Leader
		The team lead would be Accountable: Being held accountable for the RFP implementation and shall ensure seamless services.	Demonstrated service delivery experience & application support experience, preferably in a 24x7 environment
		Ensure Fair and Timely Reporting	Experience in the use of an issue Logging, assigning and tracking system (Ticketing System)
			Effective computer skills; Microsoft Office
			Effective communication skills both verbally and in writing.
			Experience of ITIL practices
			Coordination with all technical teams for troubleshooting and RCA
2	IT Help Desk Executive	Incident Management - Logging of calls from Users, departments and other engineers, raise tickets assign it to engineers	Minimum 3 years of relevant experience
		Follow-up for call closure and escalate wherever necessary. RFO to be ensured.	Experience in IT helpdesk services
		Share incident/problem report on daily,	Basic understanding of computer technology in a business environment.

		weekly and monthly basis.	Effective computer skills; Microsoft Office
			MS outlook Email client, Helpdesk / Ticketing software applications.
			Effective communication skills
			Knowledge of ITIL processes
3	System Administrator Windows, Linux, AIX	Installation, configuration, monitoring, fine tuning, troubleshooting of servers and VDI Infrastructure	1. Relevant Experience - 5 years
		Prepare & share availability reports with NABARD core IT team	2.Degree/Diploma in Computer Engineering, MCSE Certified, CCNA, RHCE, IBM AIX Administrator
		VM creation and Management	3. Experience in Windows Server 2008, 2012, 2016, 2019 and upcoming Versions Windows 10, 11 and upcoming Versions RHEL, CentOS, Ubuntu, Debian 7, 8, 9 and upcoming Versions. AIX v7 and above.
		Physical server setup and troubleshooting. He Should be well versed with DHCP, DNS, WINS, WSUS SMTP, PO3 RAS VPN SAN, Cluster environment, Back up etc.	4. Wide range trouble shooting skills involving, OS, Active Directory, LDAP, storage, security, DNS/ DHCP, DFS, printers, network, database, webserver management apache, tomcat, Jboss, IIS, Nginx, weblogic, websphere etc.
		Patch management OS, DB, servers, desktops, devices, BIOS, switches, firewalls, IOS, firmwares	5. Experience in Hyper-V, ESXi, Nutanix AHV, KVM hypervisors
		Enterprise Antivirus Updates and Patches.	6. Experience with tower, Blade and Rack mounted workstations,

		Email ID Creation & backup	7. Experience with thin clients (setup, configuration, and management)
		Complete backup of Data and Device configurations	8. Experience managing, monitoring, scaling, and implementing large enterprise level virtual desktop and application virtualization environments.
		Identification and resolution of individual and system issues which result in or potentially result in disruption to services provided	9. Experience with disaster recovery of Microsoft Active Directory and Windows and Unix Servers
		Participate in internal and external projects, reactive and proactive maintenance, sustaining, RCA and break-fix activities	10. Knowledge of storage technologies (NFS and iSCSI SAN, NAS)
			11. Linux (Suse, Red Hatt) Support
			12. Cisco/Virtualisation (Server & Desktop)
			13. Knowledge of storage technologies (NFS and iSCSI SAN, NAS), Linux (Suse, Red Hat, Ubuntu, AIX) support and Cisco/Brocade, Virtualisation (Server & Desktop)
4	DBA Personnel - Oracle, MySQL	The role will be Database Administration, installation, replication, clustering, Troubleshooting and performance tuning of databases components, taking regular backups on windows, linux and AIX.	BE/BTech/MCA

		Duties include but are not limited to Maintenance/ administration of the database	Total experience: Minimum 5 years of post-qualification experience in Database management in Oracle DB 11g ,12c, 19c and higher. MySQL 7,8 and latest Relevant Database administration certified. Oracle certified DBA (OCP)
		Space management/user management	Relevant Database administration certified
5	DBA Personnel - MS SQL	1. The role will be Database Administration, Troubleshooting and performance tuning of databases components, taking regular backups	BE/BTech/MCA
		2. Duties include but are not limited to Installation, replication, clustering, Maintenance/ administration of the databases	Total Experience: Minimum 5 years of post-qualification experience in Database management in MS SQL Server 2012,2014, 2016, 2019 and higher.
		3. Space management/user management	Relevant Database administration certified. Microsoft Certified DBA (MCDBA)
6	Nutanix Administrator	Installation maintenance and management of Nutanix clusters	Nutanix certified professional (NCP MCI 5)
			Should have hands-on experience of 4 Years on Nutanix cluster installation, monitoring, maintenance and management
			VM Replication, Flow, LEAP, Xplay, disaster recovery.
7	Security Support	Refer Scope of Work.	1. BTech, B.E. / Graduate with relevant Experience - 2 years Fortinet Certified Network

			Security Administrator (FCNSA)
			2. Certified Forcepoint NGFW Administrator
			3. Check Point Certified Security Administrator (CCSA)
			2. Hands on experience in Maintaining a PSS environment.
			3. Hands-on experience on Firewall devices, VLAN, Proxy
			4. Reporting skills & good interpretation skills
			5. Excellent communication skills
			6. Knowledge on Network Security protocols
8	Network Engineer	Refer to Scope of work.	1. B Tech / Graduate in Computer Engg, E&C or Computer Application. , CCNA is compulsory. Juniper Networks Certification Program (JNCP), JNCIA-JunOS
			2. Total 2 years should be working as Network Engineer. Hands-On experience on big multisite LAN and WAN network.
			3. Should be able to solve all the monitoring part mentioned under Scope of work and should be able to act as first point of support for all DC/DR/HO/RO calls.
9	Backup Executive	Configure new backup, Monitor and manage backup operations. Restore data on requirement.	B Tech, B.E. / in Computer Engr E&C or equivalent. Hands-on experience on high-end storage and tapes. Hands-on experience on HPDP and Arcserve backup. Minimum of 3 years' experience is required in the relevant area.

10	Regional / Corporate Office Service Support Engineer	Desktop/Laptop on-site and phone support	1.Travelling to branches / ITSM Service Provider sites within the region would be involved with this position
		Printer/Scanner support	2.Minimum 1 years of relevant experience
		Backup system support- Updating current infrastructure	3.Desktop and Network Troubleshooting
			4.Installing and configuring Operating Systems (Windows7, 8.1, 10, 11, Linux) Installing and configuring Application Software (MS Office, Open Office, .net and Java, email clients, all client software, etc.)
		VC support	Engineers should be able to manage/operate legacy VC services/MS Teams/Webex etc. from Mumbai location to various regional offices/ training establishments of NABARD
		Deploying new equipment	5.Installation and configuration of all applications Configuration of printers, scanners, projectors
		Provide investigation, diagnosis, resolution and recovery for hardware /software problems	Graduation, Diploma in any discipline. Certifications: CompTIA Network+, Network 5 Certification, Microsoft Certified Desktop Support Technician (MCDST) Microsoft Certified System Administrator windows 10 (MCSA) Two Years hands-on experience in installation and troubleshooting of windows operating system, application software's, peripheral

			devices and networking devices. Hands-on experience of basic networking. Working knowledge of ticketing system, ticket resolution and follow-up Working knowledge of online meeting setup and video conferencing. Good verbal and written communication.
		Maintain overall ownership of user's issue & service ensuring that they receive resolution within a stipulated timeframe	
		Manage service requests, software installations, new computer setups, upgrades, etc.	
		Record incident resolutions in the Help Desk tool.	
		Provide enhancement request feedback to IT regarding technology environment and customer needs through the defined processes.	
		Support the following technologies: Windows 10,11 Microsoft Office 365 products - Outlook, Word, Excel, Access, Internet Explorer, etc. desktops, laptops, printers, networked copiers, basic LAN/WAN connectivity and others as assigned.	
		Monitor daily backups.	

		Please refer scope of work	
		All relevant components in SoW	
11		Installation and troubleshooting of windows 7, 8, 10, 11 etc Install application softwares, updates, upgrades of endpoints. Monitor daily backups. Installation and troubleshooting of printers, copiers, scanners, plotters, projectors, webcams, switches, firewall, UTM, video conferencing devices etc. Install new devices, log tickets for AMC support. Resolve day to day user and network issues and improve user experience. Provide onsite support to senior officials	

Note: The qualifications and skill sets outlined above are minimum expectations only. Depending on the roles and responsibilities needed under a service domain, the engineer/s should have additional qualifications/skill -sets. All certifications should be active for next 2-5 years.

3.18. General

3.18.1. Service period: NABARD intends to avail these services for a period of 5years and extendable by 1 year.

3.18.2. Knowledge Transfer and Handshake between existing and new ITSM Service Provider will be of maximum 2 months from date of PO.

3.18.3. ITSM Service Provider will be responsible for all changes as per "Change Management Process" (Given in Annexure).

3.18.4. All resources will be appointed after screening / interview by NABARD.

3.18.5. NABARD has right to change any resources deputed by ITSM Service Provider, replacement of any such resource should be completed in 30 days from the date of intimation by NABARD.

3.18.6. NABARD will conduct quarterly review performance of all resources deployed by ITSM Service Provider. If performance of any resource is not satisfactory, ITSM Service Provider will replace of any such resource within 30 days from the date of intimation by NABARD.

3.18.7. All changes in ITSM resources should be informed to NABARD one month in advance and NABARD will be part of all handover activities.

3.18.8. The ITSM Service Provider shall provide complete services as per the scope including mounting, unmounting, installation, implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.

3.18.9. The ITSM Service Provider shall ensure that during various phases of implementation, the performance, security, network availability, etc. of the existing network setup should not be compromised.

3.18.10. ITSM Service Provider shall provide a well-maintained Documents to NABARD

3.18.11. The ITSM Service Provider shall support for replacement and upgradation of out-of-support, out-of-service, end-of-life (EOL), end of support (EOS) undersized infrastructure elements as soon as the respective OEM announced the same at no additional cost to the bank throughout contract period. The ITSM Service Provider shall inform NABARD within 15 days of announcement.

3.18.12. The list mentioned above is the indicative list; however, the successful ITSM Service Provider should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the Bank.

3.18.13. The ITSM Service Provider shall adhere to the Service Level Agreements (SLA) and regular monitoring and reporting it to the bank.

3.18.14. The ITSM services should be compliant with Bank's IT, IS, e-mail and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.

3.18.15. The ITSM processes should comply with RBI cyber security circular no. RBI/2015-16/418 dated 2 June 2016 and its annexure 1- Baseline controls(including all relevant circular and update to same by RBI).

3.18.16. The ITSM process should be of ITIL 4.0 processes for Bank requirements related to change, incident, problem, configuration management, SLA and capacity management etc.

3.18.17. The ITSM Service Provider should follow a standard process to ensure that proposed solution meets functional, security performance and regulatory requirements of the bank. The selected ITSM Service Provider shall be responsible for proactive health monitoring of infrastructure on 24x7x365 basis.

3.18.18. The Bank has a complex infrastructure with multiple resources maintained and managed through multiple ITSM Service Providers. The ITSM Service Provider shall coordinate with all other ITSM Service Providers for seamless integration, implementation and operations

3.18.19. The ITSM Service Provider shall prepare the SOPs (Standard Operating Procedures) with periodical review as per industry practices and regulatory guidelines. The drafted SOPs shall be submitted to the Bank for its review and Approval.

3.18.20. The ITSM Service Provider shall configure the SLA Levels for all applications (including hardware & software) in IT Service Management tool with the functionality of auto-escalation of incident/ticket to appropriate bank authorities in case of breach of defined timelines for resolution of incident/ticket.

3.18.21. The ITSM Service Provider shall integrate all Bank assets (Servers, Storage, Network devices) in the monitoring tools and provide the unified Dashboard for monitoring & Management of devices.

3.18.22. The ITSM Service Provider shall be responsible for patching of Bank managed servers, all desktops connected in Bank network as per frequency of patches released by product OEM.

3.18.23. The ITSM Service Provider shall ensure patching & hardening for all Bank managed servers, and get the same cleared from the Information Security Cell /SOC of the Bank. The ITSM team has to prepare a patching calendar as per the frequency of the patch released by the OEM team and share the same with the bank team. The patches have to be applied in the same month in which OEM has released the patches as per prescribed as defined in SLA.

3.18.24. The ITSM Service Provider should retain all logs including DHCP and security logs for a period of 02 years, quarterly backup of all logs including logs from tools should be provided to NABARD.

3.18.25. For any incident, Service Request, VAPT/Audit/NAC – The project manager may co-ordinate with all stakeholders in order to follow up for closure of all observations.

3.18.26. Patching support for all components of all installed & authorised software, OS patches, antivirus patches and BIOS updates.

Special Note:

3.18.27. 24 x 7 Support requirement with combination of onsite & offsite support. Onsite support is required for General shift(9AM to 6 PM) during normal working days. Support for remaining period is required on a call or remote basis. In case the issue cannot be resolved remotely, the SME (Subject matter expert) is expected to travel to our site for support.

3.18.28. VAPT support and compliance management (Review, General)

3.18.29. If required, for all scheduled and troubleshooting activities onsite engineers should be available on Saturdays/Sunday/Holidays

3.19. Miscellaneous services

ITSM Service Provider will provide following miscellaneous services:

3.18.1. In the event of shifting of office premises / Data Centers / Disaster Recovery Centers / Near Disaster Recovery Centre by the Bank, ITSM Service Provider would depute Facility Managers / engineer(s) for de-installation of all the hardware, coordinate with 3rd party vendors, supervise packing/transportation and installation/ commission of equipment at new location. No extra cost will be borne by the Bank for the same. However, packing and transportation will be arranged by the Bank separately.

3.18.2. In the event of adding new office at new locations by the Bank, ITSM Service Provider has to assist the Bank in setting up of LAN (cabling, I/O fixing etc.) coordinate with network vendor for setting up of WAN connectivity etc. Cost towards raw material will be borne by the NABARD. As & when the Bank opens its new office it is the responsibility of the ITSM Service Provider to provide ITSM engineer on call basis as per the contracted rate.

3.18.3. Suggestions/ Recommendation to improve the current infrastructure architecture for better response & security.

3.18.4. ITSM Service Provider shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed in the Bank. The Bank will provide the list of all the authorized software and the number of licenses procured.

3.18.5. If Bank implements any project in future, then the ITSM Service Provider shall provide required support.

4.2 Change in Scope

NABARD may, depending on its strategic and business requirements, decide to make modifications, alterations and additions from time to time to the Project, Services, or Deliverables of the Project. In such an event, NABARD shall provide a detailed proposal to the ITSM Service Provider specifying such requested changes ("Change Request"). ITSM Service Provider shall evaluate each Change Request. The rates and charges payable for executing the Change Requests shall be determined on pro-rata basis as per the rates used to determine the Contract Price. Based on this calculation, the ITSM Service Provider shall submit to NABARD, a written response indicating time and cost for such Change Request within 3 (three) Business Days following receipt thereof ("Change Request Response"). ITSM Service Provider's Change Request Response shall include a statement of the availability of the ITSM Service Provider's personnel and resources, as well as any impact the proposed changes will have on the Contract Price, Deliverables of this RFP or the Contract, as the case may be. NABARD, if necessary, through a designated committee, may use its reasonable efforts to accept, reject, or propose modifications to each such Change Request Response within 15 (fifteen) Business Days following receipt thereof. The ITSM Service Provider shall agree to co-operate with such committee, and furnish any further information as may be required by the committee to accept, reject or propose modifications to the Change Request Response. Upon acceptance by NABARD of a Change Request Response, the Services, Deliverables, and/or Project shall be amended by means of a written, jointly executed addendum to the Contract, which shall be considered as an integral part of the original Contract. In the event NABARD rejects a Change Request Response, NABARD shall be entitled to appoint or engage any third party service provider in repsect of the Change Request. The ITSM Service Provider shall agree to co-operate with such third party service provider.

Any Upgrade or Enhancement in relation to the IT Serivces Mangement or any AMC Services required to be rendered by the ITSM Service Provider shall not be deemed to be modifications, alterations and additions to the Project, Services, or Deliverables of the Project requiring a Change Request to be made by NABARD. All Upgrades, Enhancements and AMC Services shall be undertaken by ITSM Service Provider at its own cost, as per the terms hereof.

Since the Contract Price is determined mutually by parties, any payment to be made for any Change Request will be determined on a pro-rata basis as per the mutually decided Contract Price.

4.3 Executive Summary of the Bidders Response

The bidder in the Executive Summary should furnish synopsis of their responses to the RFP in not exceeding 15 pages. The bidder should give a brief write up relating to their capability, past experience as IT Services Mangement provider .

4.4.1 A synopsis of the understanding of the business requirements

A explanation of the approach, resourcse and ttols for of the proposed solution The hardware and software requriements, data models, technologies, data management, storage, backup, recovery, etc.

4.4.2 Deployment of resouecs and tools to achieve the objectives of this RFP.

4.4.3 Any other relevant recommendation that the bidder has to make.

5. Response to RFP

5.1. Bidder's Response

5.1.1. Preparation of Bids

The bidder should use the entire information furnished in the RFP including scope, detailed requirements, functional and technical specifications, other Annexures, Appendices and other terms and conditions to submit their response. The bidder is expected to examine all instructions, forms, terms, and specifications in the RFP.

The bidder has to submit the response to the RFP by way of a Bid comprised of:

5.1.1.1. Technical Bid indicating the response to the technical requirement specifications and functional requirement specifications

5.1.1.2. Commercial Bid furnishing all the relevant information as required.

The bidders should submit both Technical Bids and Commercial Bids online in https://nabard.eproc.in. The Bid either technical or commercial, submitted cannot be withdrawn / modified after submission of Bids.

Failure to furnish all information required as per the RFP or submission of Bids not responsive to the RFP in every respect will be at the bidder's risk and shall be liable for rejection by NABARD.

5.1.2. Authorized Signatory

The bidder shall submit the Bid authenticated by an authorized person from any of their offices in India, preferably from an office of the bidder located in Mumbai (a certified copy of the letter of authority/board resolution in this regard shall be furnished along with the Bid). The bidder's authorized signatory shall authenticate by sign and seal, each page of the Bid in original and photocopies including brochures / pamphlets / write-up etc. Bids with eraser / over writing / cutting are liable to be rejected. If required, the corrections can be made by scoring out entries and writing afresh and the authorized signatory should authenticate such corrections.

5.1.3. Cost of Preparing the Bids

The cost of preparing the response to this RFP and submission of the Bid will be borne only by the bidder and NABARD will not be liable for payment of any such costs, regardless of conduct or outcome of the bidding process.

5.1.4. Clarification on RFP document

The bidder shall carefully examine and understand the specifications / conditions of the RFP, intent of the RFP and seek clarifications in accordance with the RFP, if required to ensure that they have understood all specifications / conditions / intent of RFP for implementing the Comprehensive IT Services Management in total.

The bidder in all such cases should seek clarification in writing in the same serial order of that of RFP by mentioning relevant page number and clause number of

RFP and such clarifications should be sought, by submitting a list of queries as per Annexure XVIII – Pre -Bid Query Format in writing to NABARD on or before 6:00 PM on 27/05/2022.

All clarifications/queries on the RFP are to be in writing and are to be addressed to dit@nabard.org.

5.1.5. Pre Bid Meeting

NABARD shall hold a pre-bid meeting at on 31/05/2022 at its Head Office in Mumbai to clarify the queries raised by the bidders. No change in date and time will be entertained and NABARD will hold the meeting even if some bidder to chooses to be absent or are unable for any reason to be present during the meeting. No individual consultation shall be entertained and no clarifications other than those sought during or before the above meeting shall be entertained. No oral consultation other than during meeting will be entertained.

The clarifications of NABARD including the queries raised by bidder would be posted on the Bank's website (www.nabard.org) and these will be binding on all bidders and such clarifications will be deemed to form part of RFP. Bidders should note to give their responses by taking the clarifications given by NABARD also into consideration.

The response to the Bid should not carry any sections like clarifications, 'as orally told', 'to be discussed', interpretations, assumptions and/or conditions. With the submission of the Bid, the bidder acknowledges that they have carefully studied and understood the RFP in complete.

5.1.6. Addendum to RFP

NABARD may modify the RFP by issuing addenda for any reason, at any time prior to final date of submission of response to RFP. The addendums to the RFP as issued from time to time would be posted on the Bank's website (www.nabard.org) and these will be binding on all bidders and such addendums will be deemed to form part of RFP.

5.1.7. Language of the Bid

Both technical and Commercial Bids shall be submitted in English language as per this RFP.

5.1.8. Validity of Bids

The Bids shall remain valid for a period of 180 days from the last date of opening of Commercial Bids. All responses including Commercial Bids and Technical Bids would be deemed to be irrevocable and unconditional offers / proposals from shortlisted bidders and shall, if accepted by NABARD, deemed to form part of the final contract between NABARD and the selected bidder. NABARD may notify extensions of the Bid validity period, if required at its sole discretion prior to the date of Bid submission.

5.1.9. Bidder Quote / Offer

All responses received after the due date / time would be considered late and would be rejected. All response should be in English language. All responses by the shortlisted bidders to this RFP document shall be binding on such shortlisted bidders for a period of 180 days after the opening of the Commercial Bids or such other timeframe as may be notified by NABARD prior to the Bid submission date. Bidders are requested to attach a letter from an authorized signatory attesting the veracity of information provided in the responses. Unsigned responses would be treated as incomplete and are liable to be rejected.

Bidders are required to quote for all the components mentioned in the section 'Scope of Work' of this document. In case the bidders do not quote for any of the components, the response would be deemed to include the quote for such unquoted components.

NABARD reserves the right not to permit changes in the technical specifications and not to evaluate the offer in case of non-submission of technical details in the required format or partial submission of technical details.

5.2. Submission of Bids

5.2.1. Online Bid

Technical Bid containing documents supporting eligibility criteria (Annexure III) along with other documents and Commercial Bids to be submitted online in https://nabard.eproc.in.

Further the bidder has to quote for all the components for the Comprehensive IT Services Management. NABARD may at its discretion wherever beneficial, procure licenses for some software separately, based on any existing agreements entered into for purchase of such software.

5.2.2. Earnest Money Deposit

5.2.2.1 The earnest money deposit ("EMD") should be furnished through:

5.2.2.1.1 Remittance to NABARD Account, details of which are as under:

Name of Account	NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT
Bank Name	NABARD
Branch Name	HEAD OFFICE, MUMBAI
IFS CODE	NBRD0000002
Account Number (VAN)	NABADMN07

The UTR No for this transaction has to be indicated in the Bid Document.

-- OR --

5.2.2.1.2 Bank Guarantee (BG) from a Scheduled Commercial Bank valid for a period of 6 months from the last date of submission of Bid and strictly in the format as prescribed in Annexure - VIII.

5.2.2.2 No interest will be payable on EMD under any circumstances

5.2.2.3 Submission of EMD deposit proof in other than Technical Bid cover is entirely at the risk of the bidder and in all such cases the Bid is liable to be rejected on grounds of non-submission of EMD.

5.2.2.4 The Technical Bid will be evaluated only for those bidder who submit EMD deposit proof.

5.2.2.5 The EMD of the bidder not qualified under Technical Bid will be returned within 15 days after opening the Commercial Bid of the technically qualified bidder. The EMD of qualified bidder will be returned upon the selected bidder signing the contract and furnishing the Performance Bank Guarantee.

5.2.2.6 The EMD may be forfeited or the Bank Guarantee may be invoked if bidder withdraws its Bid during the period of Bid validity specified in the RFP; OR

5.2.2.7 Bidder having been notified of acceptance of its Bid by NABARD during the period of Bid validity:

- **a.** Fails or refuses to execute the agreement if required; or
- **b.** Fails or refuses to furnish the performance security, in accordance with the conditions of contract executed
- **c.** Offers made without the EMD will be rejected.

5.2.3. Compliance Statement

The Bidder shall certify the compliance or deviation of all clauses, terms, conditions and specifications stipulated in the RFP

Non submission of duly filled & signed Compliance Statement will make the Bid liable for rejection.

5.3. Opening of Bids

5.3.1. Opening of Technical Bids

5.3.1.1. The Technical Bid shall be opened in the presence of bidders on 17/05/2022 at 3:30 pm at NABARD Head Office, Plot C-24, 'G' Block, Bandra-Kurla Complex, Bandra (East), Mumbai - 400 051. The bidder representative may be present during the Bid opening at our office address mentioned above well in time along with authorization letter from the company.

5.3.1.2. The bidders may note that no further notice will be given in this regard. Further, in case NABARD does not function on the aforesaid date due to unforeseen circumstances or holiday then the Bid will be accepted up to 3:00 pm on the next working day and the Bids will be opened at 3:30 pm, at the same venue.

5.3.1.3. Date & time for opening of Technical Bid can be changed by NABARD without assigning any reason whatsoever. In case there is a change in the schedule the same will be intimated to the bidders by publishing on the

NABARD's website for enabling them to be present during the Bid opening.

6. Information to bidders

The bidders are expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its Bid and will be at the Bidder's own risk.

6.1. Pre-bid Meeting

6.1.1. The Bank shall hold a pre-bid meeting on the date and time mentioned in **'Critical Information'** section above. Purpose of the meeting is to bring utmost clarity on the scope of work and terms of the RFP being floated. The bidders are expected to use the platform to have all their queries answered. Considering the need to adhere to social distancing protocols amidst the Covid19 Pandemic, Pre-bid meeting may be online/offline.

6.1.2. It would be the responsibility of the bidders representatives (maximum of two person per bidder) to be present at the meeting.

6.1.3. Clarification sought by bidder should be made in writing (Letter/E-mail), as per Pre Bid Query Format (Annexure XVIII) and submitted on or before the date as indicated in the Critical Information sheet. Bank has discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting but shall not be obliged to do so.

6.1.4. The text of the clarifications asked (without identifying the source of enquiry) and the response given by the Bank, together with amendment / corrigendum to the bidding document, if any, will be posted on the Bank's (www.nabard.org) website after the pre-bid meeting on or before the date as indicated in the Critical Information sheet. It would be responsibility of the bidder to check the websites before final submission of Bids.

6.2. Amendment to the bidding document

6.2.1. Change, if any, to the bidding document at any time prior to the date of submission of bids will be notified on our website and reasonable timeframe as considered necessary may be afforded.

6.2.2. The Bank, at its discretion, may extend the deadline for the submission of Bids.

6.2.3. The amendment will be posted on Bank's website **(www.nabard.org)** and the Central Public Procurement Portal and shall be deemed to form part of the RFP**.**

6.2.4. All bidders should ensure that such clarifications/amendments have been considered by them before submitting the Bid. Bank will not have any responsibility in case of any bidder not having considered or perused the clarifications/amendments.

6.3. Language of Bid

The Bid prepared by the bidders as well as all correspondence and documents relating to the Bid exchanged by the bidder and the Bank and supporting documents and printed literature shall be in English.

6.4. Documents Comprising the Bid

The Bid shall consist of minimum eligibility criteria, Technical Bid and Commercial Bid and supporting documents as required by the RFP.

6.5. Bid Currency

Bids should be quoted in Indian Rupees only.

6.6. Earnest Money Deposit (EMD)

6.6.1. All the responses should be accompanied by a refundable INTEREST FREE security deposit of requisite value as specified in **"Critical Information"** section of the RFP.

6.6.2. EMD should be in the form of online transmission:

6.6.2.1. Remittance to NABARD Account, details of which are as under:

Name of Account	NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT
Bank Name	NABARD
Branch Name	HEAD OFFICE, MUMBAI
IFS CODE	NBRD0000002
Account Number (VAN)	NABADMN07

The UTR No for this transaction has to be indicated in the Technical Bid Document.

OR

6.6.2.2. Bank Guarantee (BG) from a Scheduled Commercial Bank valid for a period of 6 months from the last date of submission of Bid and strictly in the format as prescribed in Annexure - VIII.

6.6.3. Any Bid received without EMD in proper form and manner shall be considered unresponsive and rejected.

6.6.4. The EMD amount / BG of all unsuccessful bidders would be refunded immediately upon happening of any the following events:

6.6.4.1. Issue of LoI / purchase order to the successful bidder; **OR**

6.6.4.2. The end of the Bid validity period, including extended period (if any); **OR**

6.6.4.3. Receipt of the signed contract from the selected bidder; **whichever is earlier.**

6.6.5. Successful bidder will be refunded the EMD amount / BG only after acceptance of the Comprehensive IT Services Management by NABARD and submission of Performance Bank Guarantee by the bidder.

6.6.6. In case the acceptance of Comprehensive IT Services Management is delayed due to any reasons beyond the Bank's purview, successful bidder shall have the validity of BG towards EMD, extended for a period of three months till the Comprehensive IT Services Management is accepted by the Bank.

6.6.7. The Bid security (EMD) may be forfeited:

a. If a bidder withdraws its Bids during the period of Bid validity.

b. If a bidder makes any statement or encloses any form which turns out to be false/ forged/ incorrect at any time prior to signing of the Contract.

c. If a bidder fails to submit duly filled price breakup as per format given in Annexure –V (Commercial Bid).

d. In case of successful Bidder, if the Bidder fails to accept the LOI / Purchase Order or sign the Contract or fails to furnish performance guarantee.

6.6.8. In all the above cases, the bidder would also be banned for a period of 3 years from subsequent bidding in any of the Bank's (NABARD) tenders RFP.

6.7 Period of Validity of Bids

6.7.1 Prices and other terms offered by Bidders should be firm for an acceptance period of 180 days from date of opening of the Commercial Bid.

6.7.2 In exceptional circumstances the Bank may solicit Bidder's consent to an extension of the period of validity. The request and response thereto shall be made in writing. The Bid security provided shall also be extended.

6.7.3 Bank, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

6.8 Deadline for submission of Bids

6.8.1 The Bids should be received by the Bank at the specified address not later than the date and time specified in "Critical Information" section.

6.8.2 The Bank may, at its discretion, extend the deadline for submission of Bids by amending the Bid documents, in which case, all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

6.9 Late Bids

Portal https://nabard.eproc.in will not allow to submit bids after the deadline will **NOT** be accepted.

6.10 Modification and/ Or Withdrawal of Bids

6.10.1 No Bid may be modified or withdrawn after the deadline for submission of Bids.

6.10.2 Bank has the right to reject any or all Bids received without assigning any reason whatsoever. Bank shall not be responsible for non-receipt / non-delivery of the Bid documents due to any reason whatsoever.

6.11 Conditional Bids

Conditional Bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained in accordance with the RFP before submission of Bids.

Deviations, if any, are to be specified as per Annexure X.

6.12 Contacting the Bank

6.12.1 Bidder shall not contact the Bank on any matter relating to its Bid, from the time of opening of Bid to the time of communication in writing about its qualification or otherwise received from the Bank.

6.12.2 Any effort by the bidder to influence the Bank in its decisions on Bid evaluation, Bid comparison may result in the rejection of the ITSM Service Provider's Bid.

6.13 Opening of Bids by the Bank

6.13.1 On the scheduled date and time, Technical Bids will be opened by the Bank Committee in presence of bidder representatives. It is the responsibility of the Bidder's representative to be present at the time, on the date and at the place specified in the RFP. The Bidder's representatives who are present shall sign a document evidencing their attendance.

6.13.2 Financial / Commercial Bids of only those Bidders who qualify the Technical Bid evaluation will be opened. A separate intimation will be sent to Bidders who qualify the Technical Bid evaluation.

6.13.3 If any of the Bidder who have submitted the Bid and are not present during the specified date and time of opening it will be deemed that such bidder is not interested to participate in the opening of the Bid/s and the bank at its discretion will proceed further with opening of the Technical Bids in their absence.

6.13.4 The bidder name and presence or absence of requisite EMD and such other details as the Bank, at its discretion may consider appropriate will be announced at the time of Technical Bid opening. No Bid shall be rejected at the time of Bid opening.

6.13.5 Unsuccessful Bidders will be informed of their position. No scores or further breakdown of the evaluation will be communicated to any unsuccessful Bidders.

6.14 Pre-Contract Integrity Pact

6.14.1 Pre-Contract Integrity Pact is an agreement between the prospective Bidder and the buyer committing the persons / officials of both the Parties not to exercise any corrupt influence on any aspect of the Contract.

6.14.2 The Bidder has to submit signed Pre-Contract Integrity Pact as per the format at Annexure IX on non-judicial stamp paper of requisite value (to be borne by the Bidder) applicable at the place of its first execution along with the minimum eligibility Bid. Bidder may kindly note that documents required on stamp paper will have to be given on stamp paper and cannot be given on the company letter head.

6.15 Documents to be submitted

6.15.1 The bidder shall submit two separate Bids for the Technical Bid and Commercial/Financial Bid with relevant supporting documents in portal https://nabard.eproc.in .

Sealing and Marking

6.15.2 The Bid shall be typed or written in indelible ink, all pages numbered and shall be signed by the Bidder's representative on whose favour Power of Attorney is issued to bind the Bidder to the Contract.

6.15.3 Relevant documents should be submitted as proof wherever necessary.

6.15.4 Faxed copies of any submission are not acceptable and will be rejected by the Bank.

6.15.5 Responses should be concise and to the point. Submission of irrelevant documents should be avoided.

6.15.6 If the Bids do not contain all the information required or is incomplete, the proposal is liable to be rejected.

Bids (Technical Bid & Commercial Bid) are to be marked under the title – Comprehensive IT Services Management – RFP No. No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022

6.16 Erasures or Alterations

The offers containing erasures or alterations will not be considered until it is duly signed and stamped by the authorized signatory. There should be no hand-written material, corrections or alterations in the offer. Technical details should be completely filled in. Correct technical information of the product being offered should be filled in. Filling up of the information using terms such as “OK”, “accepted”, “noted”, “complied”, “as given in brochure / manual” is not acceptable. The Bank may treat such offers as not adhering to the RFP guidelines and as unacceptable.

6.17 Public Procurement Policy on Micro and Small Enterprises (MSEs)

6.17.1 NABARD is governed by provisions of the Public Procurement Policy for Micro and Small Enterprises (MSEs) as circulated by the Ministry of MSME, GoI.

6.17.2 These provisions shall be applicable to Micro and Small Enterprises (MSEs) registered with District Industries Centers or Khadi and Village Industries Commission or Khadi and Village Industries Board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises (MSMEs).

6.17.3 Such MSEs would be entitled for exemption from furnishing tender fee and EMD. In case of any issue on the subject matter, the MSE’s may approach the tender inviting authority to resolve their grievances.

6.17.4 Agencies/Bidders desirous of availing exemptions/ preference under above provisions should submit a copy of proof of registration as MSEs/ and ownership of the same by SC/ST along with the tender/RFP.

6.17.5 The bidder to note that, in the current RFP splitting of order is not applicable.

6.17.6 NABARD shall be governed by the Public Procurement (Preference to Make In India) Order, 2017 – Revision dated 04 June 2020 issued by the Department of Promotion of Industry and Internal Trade, Ministry of Commerce, Government of India. Any claim of preference under the above order shall be considered subject to submission/examination of all necessary documents as envisaged under the Order.

6.18 Release from Liability

6.18.1 It shall be deemed that by submitting the Bid, the bidder agrees and releases the NABARD, its employees, agents and advisers, irrevocably, unconditionally, fully and finally from any and all liability for claims, losses, damages, costs, expenses or liabilities in any way related to or arising from the exercise of any rights and/ or performance of any obligations hereunder and in connection with the bid process, to the fullest extent permitted by Applicable Law, and waives any and all rights and/ or claims it may have in this respect, whether actual or contingent, whether present or in future.

6.19 Conflict of Interest

6.19.1 The scope of this clause only extends to the bid process and to that extent, any conflict of interest, shall fall within the scope of the provision and render the bidder ineligible.

6.19.2 No bidder shall have a conflict of interest that affects the bid process. If any bidder is found to have a conflict of interest, such bidder shall stand disqualified and NABARD shall be entitled to invoke the bid/performance security/bond, as the case may be. A bidder shall be deemed to have a conflict of interest affecting the bidding process, if:

6.19.2.1 the bidder and/or their respective Affiliates (or any constituent thereof) should not have common controlling shareholders or other ownership interest in any other bidder and/or their respective Affiliates (or any constituent thereof). However, such disqualification shall not apply in cases where:

6.19.2.2 the direct or indirect shareholding of a bidder and/or their respective Affiliates (or any constituent thereof) in any other bidder and/or their respective Affiliates, is less than 25% (twenty five per cent) of the subscribed and paid up equity share capital thereof; and/or

6.19.2.3 the ownership is by a bank, insurance company, pension fund or a public financial institution as defined under Section 2 (72) of the Companies Act, 2013 or a foreign portfolio investor.

6.19.2.4 the bidder or their respective Affiliates (or any constituent thereof) receives or have received any direct or indirect subsidy, grant, concessional loan or subordinated debt from any other bidder.

6.19.2.5 the Bidder, its Affiliate (or any other constituent thereof) have a relationship with another bidder, its Affiliate thereof, directly or through common third party/ parties, that puts either or both of them in a position to have access to each other's information about, or to influence the Bid of either or each other.

6.20. Disqualifications

6.20.1. In addition to the grounds for rejection/disqualification mentioned elsewhere in this RFP, NABARD shall have the right, in its sole discretion, to disqualify any bidder for one or more of the following grounds:

(i) declaration of any of the Bidder as ineligible due to corrupt or fraudulent practices, in any prior tender process in the past or black listing by NABARD;

(ii) the Bid not being accompanied by any supporting documents or annexes required to be submitted in accordance with the RFP;

(iii) submission by the bidder of more than one Bid or submission of a conditional Bid;

(iv) failure to comply with the requirements of the RFP or the Bid being non-responsive to the requirements of the RFP, for reasons including but not limited to the Bid not being signed, sealed or marked as stipulated in the RFP, not containing all the information as required in the RFP or in the format as specified in the RFP;

(v) failure to furnish the EMD as per the RFP;

(vi) if the Bid contains incorrect/ inaccurate/ incomplete/ misleading information or if the Bid contains any misrepresentation;

(vii) if the bidder has not paid any of its dues payable to NABARD which have become payable on or before submitting the Bid;

(viii) there is a conflict of interest as specified in Clause 6.19 above and/or

(ix) a Bid is submitted beyond the deadline specified in the RFP.

****

7. Minimum Eligibility Criteria

7.1. The Bidder should satisfy the Minimum Eligibility Criteria as per Annexure-III of the RFP.

7.2. The bidder should comply with all the above mentioned criteria. Non-compliance of any of the criteria will entail rejection of the Bid summarily. These criteria are mandatory.

7.3. Only those who fulfill all the eligibility criteria will qualify for further evaluation.

7.4. Copies of relevant documents / certificates duly attested by authorised signatory and company seal affixed should be submitted as proof in support of the claims made. The Bank reserves the right to verify / evaluate the claims made by the bidder independently.

7.5. Reference Customer Name and Contact information to be provided to the Bank with whom discussion can be done.

8. Evaluation Methodology

8.1. Evaluation Process will be in 3 phases and will be based on the following three criteria.

- Minimum Eligibility Criteria
- Technical Bid
- Commercial Bids

8.2. NABARD shall evaluate first the 'Eligibility Criteria' bids and based on its evaluation, 'Technical Bids' shall be undertaken only for those bids that clear this stage. Subsequently Commercial bids shall be opened for only those bids clearing the technical evaluation.

8.3. Minimum eligibility Criteria

8.3.1. Bids submitted by all the Bidder would be evaluated for eligibility asper the parameters mentioned Annexure III. Bids not complying with any of the Minimum eligibility criteria are liable to be rejected and will not be considered for further evaluation. Only Successful bids out of this stage would be considered for technical evaluation.

8.3.2. Bidders may ensure to submit all required documents as per requirements and as indicated in Annexure III as no further opportunity for submission of additional documents would be given and bids without verifiable facts would not be considered.

8.4. Technical Evaluation

8.4.1. The technical bids would be evaluated on the basis of responses by Bidder to the detailed scope of work .

8.4.2. NABARD reserves the right to seek specific clarifications from any or all the Bidder(s) at this stage. All the clarifications received within the stipulated time shall be considered for evaluation. In case satisfactory clarifications are not received from the Bidders within the stipulated time, the respective technical parameters would be treated as non-compliant.

8.5.2. Technical bids would be evaluated on the following broad parameters:

S. No.	Parameter	Weightage
A	**Technical Parameters**	**50%**
1	Annual Maintenance Contract (AMC)	100 Marks
2	Desktop Management	
3	Online Asset tracking and Inventory Management tool	
4	Patch Management using the tool	
5	Domain Services Management	

6	File Services Management	
7	Storage Management	
8	Data Center and Server Management	
9	Network Management Services	
10	IT Security Management	
11	Data Base Administration	
12	Vendor Management	
13	Help/Service Desk Services Management	
14	Non-Delivery of Services / PENALTIES & SLAs	
15	Covering for Absence of ITSM Services	
16	Staffing/Skill-Set/Qualification/Experience/Knowledge Sharing	
17	General	
18	Miscellaneous services	
B	**Presentation**	**20%**
C	**References / Site Visit**	**20%**
D	**Own Geographical Spread**	**10%**
	Total	**100%**

8.5.2. The technical bid will be evaluated and an Overall Technical Score (OTS) assigned to each bid based on the parameters mentioned above.

8.5.2. The **Overall Technical Score (OTS)** for each bidder will be calculated as follows :

$$\mathbf{OTS = T / T_{high} * 100}$$

Where

OTS – Overall Technical Score obtained by the Bidder

8.5.2. T - Technical score obtained by bidder

T_{high} - Highest Technical score secured among the Bidders

8.5.2. Technical Bids receiving an OTS greater than or equal to a score of 75 (cut-off marks) will be eligible for consideration in the subsequent round of commercial evaluation.

8.5.2. If less than 3 Bidders qualify as per above criteria NABARD reserves the right to short list maximum top 3 Bidders subject to OTS >= 70.

8.5.2. Overall Technical Score (OTS) of the technically qualified bids would be announced before the representatives of the Bidders and only the commercial bids of those Bidders would be opened for commercial evaluation.

8.5. Commercial Evaluation

8.5.1. Only the Bidders who are found technically qualified in Technical Evaluation will be taken for commercial evaluation.

8.5.2. The date for opening of commercial bids will be separately advised.

8.5.2. The Net Present Value (NPV) method would be used for calculating the final value, quoted for all five years, to arrive at derived commercial bid value for evaluation. [NPV formula of Microsoft Excel Worksheet shall be used for the purpose].

8.5.2. Discount rate will be considered by bank as 7.25% (for calculation of NPV).

8.5.2. The eligible bidder will be selected based on NPV L1 thus obtained.

8.5.3. The Bidder, based on final weighted evaluation score calculated in the ratio of technical 80% and commercial 20% is found to be the Highest, will be selected for further discussion for finalizing contract / placing PO or LOI subject to satisfying all the terms and conditions defined in this RFP document

8.6 Objectives of the Evaluation Methodology

8.6.1. The objective of the evaluation process is to evaluate the Bids to select a capable and best fit bidder at a competitive price. The evaluation by NABARD will be undertaken by TEC. The bidder will make presentation to the TEC. The decision of the TEC shall be considered final.

8.6.2. The 'Technical Bid' will contain the exhaustive and comprehensive technical details whereas the 'Commercial Bid' will contain the pricing information. The Technical Bid shall NOT contain any pricing or commercial information at all and if the Technical Bid contains any price related information, then that Technical Bid would be disqualified and would NOT be processed further.

8.6.3. In the first stage, only the 'Technical Bids' will be opened and evaluated. All eligible Technical Bids will be evaluated, and a technical score would be arrived at. The bidder scoring 70 per cent and above in technical evaluation will be qualified for Commercial Bid opening.

8.6.4. In the second stage, the Commercial Bids of only those bidder shall be evaluated who have qualified in the technical evaluation. The remaining Commercial Bids, if any, shall not be opened.

8.6.5. Final weighted evaluation score will be calculated in the ratio of technical 80% and commercial 20%.

8.6.6. NABARD may call for any clarifications/additional information required, if any, on the Bids submitted. The bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The Bidder's offer may be disqualified, if the clarifications/ additional sought by the Bank are not submitted within the specified date and time.

8.6.7. NABARD reserves the right to call for presentation/s etc., from the Bidders based on Technical Bids submitted by them. NABARD also reserves the right to enquire discreetly with references provided by the Bidders regarding previous engagements undertaken by the Bidder. Based upon the final technical scoring, the eligible Bidders shall be short listed for final Commercial Bid opening.

9. Liquidated Damage

Time is essence of the Contract and NABARD expects the bidder to complete the project implementation within the period of 2 months from issuance of PO and provide services for next 60 months as per the implementation plan specified in the RFP. If the bidder fails to:

9.1. To deliver any or all Deliverables; or
9.2. To complete the installation and commissioning of the Comprehensive IT Services management as per the time schedule given in the RFP; or
9.3. To commence Services within the time specified as per the terms of the RFP; or
9.4. To perform the Services and extend the support that meets the requirements as stipulated in the RFP within the time specified in the RFP; or

NABARD shall without prejudice to its other rights and remedies under and in accordance with the terms of RFP levy liquidated damages from payments due to the Service Provider. Inability of the Service Provider to the provide requirements as per scope or to meet the timelines as specified would attract liquidated damages and shall be entitled to invoke the guarantees furnished by the bidder to the extent of the liquidated damages applicable.

Except as otherwise provided under the SLA for any non-performance or delay in performance of obligations by the ITSM Service Provider, if the Service Provider fails to deliver any or all of the Deliverables or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent of total Contract Price per week of delay until actual delivery or performance, subject to maximum deduction of 10% of the total Contract Price and shall be entitled to invoke the guarantees furnished by the bidder to the extent of the liquidated damages applicable.

The liquidated damages are to be calculated on the Contract Price.

NABARD reserves the right to recover the liquidated damages from any payment to be made under this Contract for Comprehensive IT Services management. The liquidation damages represent a genuine pre-estimate of the loss or damage that NABARD may suffer due to delay or breach in performance of the obligations by the ITSM Service Provider.

It is further clarified that :

i. NABARD has the right to enforce liquidated damages by way of set off.
ii. Overall liability will be calculated as per applicable laws.
iii. NABARD cannot take the responsibility of establishing the reasons for delay, unless delay is attributable to *force majeure* event, which is provided for under the RFP, the delay shall attract liquidated damages.

10. Special Terms and Conditions

10.1. Duration of Contract

10.1.1. The Business Requirements Document needs to be prepared in consultation with the NABARD within 1 month of the award / signing of the Contract. The Comprehensive IT Service Mangement should start proving services within 1 months from the completion of Business Requirements Document. However the total period to Comprehensive IT Service Mangement implementation should not exceed 2 months from the date of award / signing of the Contract.

The timelines for the purpose of the contract are detailed under para 10.9.1.

10.1.2. Bank will enter into a contract with the selected bidder initially for a period of 5 years commencing from the date of signing of the Agreement between NABARD and the selected ITSM Service Provider. However, the same should be extendable with maximum upto extensions of 1 year or part thereof, if the Bank so desires based on mutual agreement.

10.1.3. The Bank will reserve a right to re-negotiate the price and terms of the entire Contract with the selected bidder at more favorable terms in case such terms are offered in the industry at the time of extension of Contract

10.1.4. Bank reserves the right to terminate the Contract by providing a written notice of 3 months to the selected ITSM Service Provider

10.2. Award and Signing of Contract

10.2.1. Selected bidder would be issued Purchase Order (PO) on final selection and completion of internal approval formalities of the Bank. At any time prior to issuance of the PO, NABARD reserves the right to accept or reject any Bid and to annul the bid process, without incurring any liability to the affected bidder or any obligation to inform the affected bidder of the grounds for NABARD's action. The bidder shall not be entitled to make any claim against NABARD on account of such rejection or annulment.

10.2.2. The selected bidder has to return the duplicate copy of the PO along with NDA (as per format given in Annexure –XIII of the RFP) within 7 working days, stamped and signed by Authorized Signatory as token of acceptance.

10.2.3. The selected bidder will be required to begin execution of the work within 45 days from the date of signing of the contract.

10.3. Price

10.3.1. Prices quoted by the Bidders should be inclusive of all local taxes, GST, duties, levies, transportation costs etc..

10.3.2. Once a Contract Price is arrived at, the same should remain firm and should not be subject to escalation during the performance of the Contract due to fluctuation in foreign currency, changes in costs related to the materials and labour or other components or for any other reason.

10.3.3. Bidder will be entirely responsible for all applicable present and future, duties, levies, charges, license fees etc. in connection with delivery of goods / Services at site including incidental services and commissioning.

10.3.4. While any increase in the rates of applicable taxes or impact of new taxes imposed by the Central or State Governments of India, subsequent to the submission of commercial Bid shall be borne by NABARD, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to NABARD in its favour. This will remain applicable throughout the Contract Period.

10.3.5. No other cost whatsoever will be paid by NABARD.

10.4. Payment Schedule

10.4.1. The cost shall be paid by NABARD on quarterly basis at the end of each quarter on receipt of valid invoices raised by the ITSM Service Provider/selected ITSM Service Provider.

10.4.2. The Bank shall only make payments after discounting any penalties that may be imposed on the selected ITSM Service Provider for breach of any Contract terms as per SLA.

10.4.3. No additional payment apart from the Commercial Bid value will be done under any circumstances.

10.4.4. All payments will be made by adopting electronic clearing system and electronic fund transfer.

10.4.5. Deduction of Income Tax, Goods and Services Tax and other applicable statutory duties would be as per the extant laws.

However, NABARD would ensure payment within 30 working days in respect of the Invoices which are complete in all respects.
The payment schedule proposed is standard and cannot be changed for the ITSM Service Provider.

10.5. Termination of Contract

10.5.1. NABARD may terminate this Agreement by giving a 90 (ninety) days prior written notice to the ITSM Service Provider without assigning any reason.

10.5.2. The Bank shall have the right to terminate the Contract with the selected ITSM Service Provider at any time during the Contract Period, by giving a written notice, for reasons, including but not limited to the following:

ii. If the ITSM Service Provider fails to deliver any or all of the Services within the period(s) specified in the Contract or within any extension thereof granted by the Bank pursuant to conditions of the Contract; or

iii. If the ITSM Service Provider fails to perform any other obligation(s) under the Contract and fails to cure such non-performance within 30 (thirty) days from date of the written notice informing the ITSM Service Provider of such non-performance; or

iv. Discrepancies / deviations in the processes and/or products agreed to be delivered by the ITSM Service Provider as per the terms of the Contract and fails to cure such discrepancy / deviations within 30 (thirty) days from date of the written notice informing the ITSM Service Provider of such non-performance; or

v. If a ITSM Service Provider makes any statement, representation, warranty or furnishes any form in relation to the Services, which turns out to be false/ forged/ incorrect at any time during the Contract Period; or

vi. Violation of terms & conditions stipulated in this RFP or under the Contract and fails to cure such breach within 30 (thirty) days from date of the written notice informing the ITSM Service Provider of such non-performance; or

vii. Failure in following security standards laid down by NABARD under the Contract.

10.6. Termination for insolvency

Upon occurrence of an event of dissolution of the selected ITSM Service Provider, whether by operation of Applicable Law or otherwise, commencement of winding up or insolvency proceedings of the selected ITSM Service Provider or assignment by the selected ITSM Service Provider for the benefit of its creditors, or the ITSM Service Provider passing a resolution for voluntary winding up, or appointment of a receiver, the ITSM Service Provider shall immediately provide a written notice to the Bank informing the Bank of occurrence of such event. The Bank may at any time subsequent to receipt of such notice from the ITSM Service Provider have the right to terminate the Contract forthwith.

The ITSM Service Provider is entitled to retain all payments made for services availed till the date of termination of the contract.

10.7. Consequences of Termination

10.7.1. In case of termination of the Contract by NABARD pursuant to Clause 10.5.1, any payments made by NABARD to the ITSM Service Provider (for period for which Services are not availed) would necessarily have to be returned to NABARD.

10.7.2. In case of termination of the Contract by NABARD pursuant to Clause 10.5.2, any payments made by NABARD to the ITSM Service Provider (for period for which Services are not availed) would necessarily have to be returned to NABARD with interest @ 15% per annum. Further, the ITSM Service Provider shall compensate NABARD for any direct Losses incurred by NABARD due to the termination of the Contract and any additional expenditure to be incurred by NABARD in appointing any other service provider for the Services.

10.7.3. In the event Bank terminates the Contract in whole or in part for any reason, Bank may procure, upon such terms and in such manner, as it deems appropriate, systems or services similar to those undelivered and the ITSM Service Provider shall be liable to Bank for any excess costs for such similar systems or services. However, the ITSM Service Provider shall continue the performance of the Contract to the extent not terminated.

10.7.4. Upon termination, the ITSM Service Provider shall ensure transition of Services and co-operate with the Bank in the manner as set out in clause 11.16.

10.8. Periodic Review & Inspection

10.8.1. NABARD shall have the right to conduct periodic review and inspection, as and when required, to review ITSM Service Provider's performance, financial stability, service reliability, and compliance with the SLA.

10.8.2. NABARD shall have the right to conduct, a periodic inspection on the systems, books and records in relation to the Project, as maintained by the ITSM Service Provider to ensure quality control and compliance of the ITSM Service Provider with the Business Requirements Document and Technical Architecture as well delivery timelines. The inspection may be conducted by NABARD or through third party experts appointed by NABARD. In the event any deficiency is determined by NABARD pursuant to such inspection, the ITSM Service Provider shall rectify such deficiency within timelines prescribed by NABARD and shall issue of certificate of compliance to NABARD.

10.9. Project Timelines

10.9.1. The ITSM Service Provider should complete handover from existing ITSM vendor within 60 days from the **Date of signing of contract** as determined by NABARD and to be recorded under Contract and PO

10.9.2. The Bank will consider the inability of the ITSM Service Provider to deliver the Services within the specified time limit, as a breach of Contract.

10.9.3. The Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum as specified in the SLA

10.10. Acceptance

10.10.1. NABARD shall be entitled to verify and examine the Comprehensive IT Services mangement , and each program, solution, tool or other component thereof upon delivery.

10.10.2. The ITSM Service Provider shall assist NABARD in undertaking the User Acceptance Test for each Deliverable. The User Acceptance Test shall comprise of : (i) Function test (ii) robustness test (iii) integrity test (iv) capacity and response time test (v) review of all Documenation (vi) installation test and (vii) test of operating procedures, as applicable to the relevant Deliverable.

In the event any Deliverable is not in accordance with the Technical Architecture and Scope, or is defective in any way, or are otherwise not to the satisfaction of NABARD, then within 30 (thirty) days from such delivery, NABARD shall notify the selected ITSM Service Provider of the same (“**Defect Notice**”). ITSM Service Provider shall, upon receipt of such Defect Notice from NABARD, promptly and in any event no later than 4 (four) days from the date of the Defect Notice, replace the relevant Deliverable specified in the Defect Notice, at its own cost and expense. Any Deliverable delivered by the selected ITSM Service Provider to NABARD in replacement of any previously delivered Deliverable shall undergo the same process as set out above with respect to verification of defect and replacement. The results of the User Acceptance Test shall be recorded in writing.

10.10.3. The Comprehensive IT Services mangement will be accepted once the complete Comprehensive IT Services mangement is implemented at NABARD and the users are able to generate reports and run use cases as specified by NABARD. Upon acceptance, the ITSM Service Provider shall handover control and administration of the Deliverable by providing complete access and all passwords, usernames, credentials, authenticators etc., as required.

10.10.4. The ITSM Service Provider shall obtain Acceptance Certificate/s from the Bank, which would contain the date of acceptance only post fulfillment of Clauses 10.10.1. and 10.10.2 in respect of the entire ITSM Solution.

10.10.5. NABARD will not agree to a deemed approval clause.

11. General Terms and Conditions

11.1. Definitions

In this RFP / the Contract, the following terms shall be interpreted as indicated:

11.1.1. "AMC Services" shall mean annual maintenance services to be rendered by the ITSM Service Provider as listed out in Clause 4.2.1 .

11.1.2. "Applicable Law" means any law, rule, regulation, ordinance, order, code, treaty, judgment, decree, injunction, permit or decision of any central, state or local government, authority, agency, court or other body having jurisdiction over the matter or person in question, including those prevailing in the relevant jurisdiction, as in effect, from time to time;
The current definition of "Applicable Law" applies to courts, other bodies etc having jurisdiction over the matter or person in question. Therefore, the definition in its current form is applicable for each Party based on the operation of its business.

11.1.3. "Approach Document" means a document setting out the strategy and approach to design, develop, and implement and use the Comprehensive IT Services mangement by the ITSM Service Provider in accordance with the Business Requirement Document;

11.1.4. "Background Intellectual Property" means intellectual property owned or controlled by a Party, including intellectual property developed prior to or independently of this RFP or the Contract, which the Party determines, in its sole discretion, to make available for the carrying out of the Services and includes intellectual property licensed to or acquired by the Parties from time to time pursuant to this RFP and the Contract.

11.1.5. "Bank", "NABARD", "Purchaser", "Buyer" means National Bank for Agriculture and Rural Development (NABARD);

11.1.6. "ITSM Service Provider'", "ITSM Service Provider", "ITSM Service Provider", "Supplier", "Service Provider", "Seller" means the respondent to the RFP document.

11.1.7. "Business Days" means any day of the week except Saturday, Sunday or any day on which the banks in India are closed for business;

11.1.8. "Business Requirement Document" means a formal document that outlines the goals and expectations of NABARD in respect of the Project which shall be prepared by NABARD in consultation with a succesful ITSM Service Provider.

11.1.9. "Data Centre" / "DC" means data centre owned, operated, and/or controlled by NABARD, as intimated by NABARD in writing.

11.1.10. "Deliverables" means the products, infrastructure and services agreed to be delivered by the ITSM Service Provider as per the Contract as defined more elaborately in the RFP, and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc.

11.1.11. "Documentation" means the then-current technical and functional documentation for each component of the Comprehensive IT Services mangement, whether software or hardware, including, but not limited to, configuration workbooks or release notes, terms of service and policies, as applicable.

11.1.12. “RFP”. “Tender”, “RFP”, “Bid document’ means the ‘Request for Proposal document.

11.1.13. “Confidential Information” means all information that NABARD designates as being confidential or which the circumstances surrounding the disclosure ought to be treated as confidential. It includes all information disclosed / furnished by NABARD or any such information which comes into the knowledge of the ITSM Service Provider during the course of engagement, whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the ITSM Service Provider to carry out the assignment, and shall mean and include, without limitation (1) data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; (2)information relating to installed or purchased Disclosing Party material or hardware products, the information relating to general architecture of Disclosing Party’s Comprehensive IT Services mangement, information relating to nature and content of data stored within Comprehensive IT Services mangement or in any other storage media, Disclosing Party’s business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement; (3) Information such as any trade secrets, discoveries, ideas, concepts, techniques, materials, formulae, compositions, information, data, results, plans, surveys and/or reports of a technical nature or concerning research and development and/or engineering activity, commercial, financial, scientific or technical information, patent and trademark applications, process designs, process models, drawings, plans, designs, data, databases and extracts there from, formulae, methods, know-how and other intellectual property, marketing and pricing information, and other strategies, concepts, ideas; (4) technical or business information or material not covered in (i); (5) proprietary or internal information relating to the current, future and proposed products or services of NABARD including, financial information, process/flow charts, business models, financial reports, business plans, customer lists, products or production processes, designs, drawings, data information related to products and services, procurement requirements, purchasing, customers, investors, employees, business and contractual relationships, business forecasts, business plans and strategies, information the Parties provide regarding third parties; (6) information disclosed pursuant to this agreement including but not limited to Information Security policy and procedures, internal policies and plans and Organization charts etc.; and (7) all such other information which by its nature or the circumstances of its disclosure is confidential Confidential Information in oral form should be identified as confidential at the time of disclosure and confirmed as such in writing within fifteen days of such disclosure

11.1.14. "Bid" may be referred to as 'Offer'.

11.1.15. "Bugs" means a failure of a software or program to perform as specified in the applicable product description and/or user's guide and/or installation guide due to defective software distribution media or otherwise

11.1.16. "Commercial Bid / Financial Bid" indicates the response by the Bidder containing all relevant information required as per response to the RFP.

11.1.17. "Contract" means the agreement entered into between the Bank and the ITSM Service Provider, pursuant to acceptance by the Bank of the ITSM Service Provider's Bid on terms as contained in this RFP, substantially in the form attached hereto as Annexure XV, and shall include all attachments and appendices thereto and all documents incorporated by reference therein including the SLA. The said form of the Contract attached as Annexure XV is an indicative agreement proposed to be executed by NABARD with the selected ITSM Service Provider, which shall be finalised at the time of execution thereof.

11.1.18. "Contract Price" means the price payable to the ITSM Service Provider under the Contract for the full and proper performance of its contractual obligations;

11.1.19. "Comprehensive IT Services mangement" means the IT Services Management Solution to be designed and developed by the ITSM Service Provider as per the Business Requirement Document provided under the Contract .

11.1.20. "Losses" means all losses, liabilities, liens, obligations, fines, costs, charges, expenses, royalties, damages (whether or not resulting from third party claims), including those resulting from claims and including interest and penalties with respect thereto and related out-of-pocket expenses paid to third parties, including reasonable attorneys' and accountants' fees and disbursements.

11.1.21. "Party / Parties" means NABARD and the ITSM Service Provider, as the context may require.

11.1.22. "Regulatory Authorities" means any government or governmental or regulatory body, or political subdivision, whether foreign, federal, state, city or local, or any agency, commission, authority, or instrumentality, any multinational, supra-national or quasi-governmental entity, body or authority, any self-regulatory organization, any court or arbitrator (public or private) thereof, or any entities that a government controls or owns (in whole or in part), including any state-owned, controlled or operated companies or enterprises

11.1.23. "Security Architecture" means a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment in respect of an information technology infrastructure.

11.1.24. "Services" means all services, scope of work and deliverables to be provided by a selected ITSM Service Provider as described in the RFP and includes services ancillary to the Comprehensive IT Services mangement, such as installation, commissioning, integration with existing systems, provision of technical assistance by the selected ITSM Service Provider training, maintenance, support, contract and other such obligations covered under the RFP and the Contract.

11.1.25. "Software Licensing Cost" means the cost incurred or to be incurred by the selected ITSM Service Provider for licensing of third party software for the purpose of the Comprehensive IT Services mangement.

11.1.26. "Technical Architecture" means a document specifying the overall plan for the Comprehensive IT Services mangement and shall include functional, infrastructure, data, deployment, network for the proposed Comprehensive IT Services mangement.

11.1.27. "Technical Bid" indicates the response by the ITSM Service Provider to the technical requirement specifications and functional requirement specifications in response to the RFP

11.1.28. "User Acceptance Test" means user acceptance testing to ensure that all features as agreed under the Contract of the Comprehensive IT Services mangement are functional.

11.2. Use of Contract Documents and Information

11.2.1. The Supplier shall not, without the Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the Supplier in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

11.2.2. The Supplier will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other Party without the prior written approval of the Bank.

11.3. Personnel and Inspection of Records

11.3.1. The ITSM Service Provider shall coordinate with the authorised representatives of NABARD, for continuous monitoring and assessment by NABARD of the Services provided under the Contract.

11.3.2. The ITSM Service Provider shall appoint sufficient number of individuals in order to ensure that the Services are provided to NABARD in a proper, timely and efficient manner. Any change in the designated team of personnel appointed for the Sevrices, shall be subject to prior written approval from NABARD.

11.3.3. The ITSM Service Provider shall maintain electronic books of accounts, log-books and any other operating records that it may deem necessary in connection with the rendering of Services under this Contract. The ITSM Service Provider shall retain all such electronic books of accounts and operating records relating to the Services for a period of 7 (seven) years after the completion of the Services or earlier termination of the Contract.

11.3.4. In order to enable NABARD to comply with Applicable Laws, the ITSM Service Provider shall furnish such documents and information, in addition to the books and electronic records maintained by the ITSM Service

Provider in terms of Clause 11.3.3 (Personnel and Inspection of Records) above, as may be requested by NABARD, from time to time, in relation to the Services rendered by the ITSM Service Provider under the Contract, provided that the cost and expenses incurred in providing such documents and information (other than books and records maintained) by the ITSM Service Provider shall be borne by NABARD.

11.3.5. During the Contract Period and thereafter, subject to receipt of advance notice of [3 (three)] Business Days from NABARD, the ITSM Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any Business Day, access its premises to inspect the electronic records maintained by the Service Provider in relation to the Project.

11.3.6. If required under Applicable Law, the ITSM Service Provider shall, during the Contract Period and thereafter, provide access to any Governmental Authority to inspect records, documents, books and accounts of the ITSM Service Provider maintained in relation to the Services rendered under the Contract.

11.4. Subcontractors

11.4.1. Subcontracting or delegation of its obligations by the selected ITSM Service Provider is explicitly prohibited, except with the prior written consent of NABARD in relation to subcontracting or delegation; and provided that the selected ITSM Service Provider shall inform such sub-contractor of the confidential nature of information, which may be shared pursuant to such sub-contracting or delegation by the selected ITSM Service Provider and procure that such sub-contractor is bound by the confidentiality obligations that are materially similar to those set out in Clause 11.22 of this RFP.

11.4.2. Unless NABARD specifically approves appointment of any sub-contractors submitted by the selected ITSM Service Provider, the request shall be deemed to have been rejected and not approved by NABARD.

11.4.3. In relation to a sub-contractor appointed in terms of this Clause 11.4.3, NABARD may, withdraw its approval and direct the selected ITSM Service Provider to terminate the appointment of such subcontractor with immediate effect or within such other period as may be prescribed by NABARD in its sole discretion, if NABARD reasonably determines that the subcontractor is in breach any terms of the Contract or if NABARD is not satisfied with the quality of Services rendered by such sub-contractor. Upon receipt of notice by the selected ITSM Service Provider, the selected selected ITSM Service Provider shall be required to terminate the appointment of such sub-contractor, provided that nothing contained in this Clause 11.4.3 shall effect the right of the selected ITSM Service Provider to appoint any other sub-contractor in terms of this Clause 11.4.3.

11.4.4. A copy of contract details entered between the selected ITSM Service Provider and the sub-contractor shall be made available by the ITSM Service Provider to NABARD within 7 (seven) days of engaging the sub-contractor.

11.4.5. Even if subcontracting by the selected ITSM Service Provider is permitted at any time by NABARD, the selected ITSM Service Provider shall be and remain responsible for all the Services provided to the Bank to the same extent as if such obligations were performed entirely by the selected ITSM Service Provider. The selected ITSM Service Provider shall be responsible for ensuring that the sub-contractor complies with all security requirements of the Contract and Bank shall have the right to obtain independent audit report for the such compliance. Duplicacy in resources due to subcontracting and related costs will be beared by ITSM service provider.

11.5. Governing language

11.5.1. The Contract shall be written in English. All correspondence and other documents pertaining to the Contract, which are exchanged by the Parties , shall be written in English.

11.5.2. The technical documentation involving detailed instruction for operation and maintenance, users' manual etc. is to be delivered with every unit of the equipment supplied / Services provided. The language of the documentation should be English.

11.6. Applicable laws

The Contract shall be interpreted in accordance with the laws prevalent in India.

11.7. Compliance with all Applicable Laws

The ITSM Service Provider shall undertake to observe, adhere to, abide by, comply with and notify the Bank about all Applicable Laws, pertaining to or applicable to the ITSM Service Provider, its business, employees or its obligations towards them, and all purposes of this RFP and the Contract. Compliance in obtaining approvals/ permissions/ licenses

11.8. Compliance in obtaining approvals / permissions / licenses

The ITSM Service Provider shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this Project or for the conduct of their own business under any Applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the Contract Period.

11.9. Performance security

11.9.1. The successful ITSM Service Provider(s) shall provide performance security in the form of a performance bank guarantee from a scheduled commercial bank for an amount equivalent to 10% of the Contract Price ("**Performance Bank Guarantee / PBG**"). The PBG should be submitted within 21 days form the execution of the Contract. If the PBG is not submitted, the Bank reserves the right to cancel the Contract.

11.9.2. The PBG shall be in force throughout the Contract Period and NABARD shall have the right to invoke the PBG during a period ending 6 months from the date of expiry / termination of the Contract.

11.9.3. Performance Bank Guarantee may be invoked in case of violation of any of the terms and conditions of the Contract or in case of deficiency / delay in implementation/Services provided by the successful ITSM Service Provider.

11.9.4. In case of extension of the Contract, the ITSM Service Provider will be required to submit a performance bank guarantee equivalent to **3%** of the Contract Price for the total extension period with additional 6 months towards invocation period.

11.10. Forfeiture of performance security

The Bank shall be at liberty to set off/adjust the proceeds of the PBG towards the loss, if any, sustained due to the the selected ITSM Service Provider's failure to complete its obligations under the Contract. This is without prejudice to the Bank's right to proceed against the selected ITSM Service Provider if the PBG is not sufficient to fully cover the loss/damage suffered by the Bank, or otherwise.

11.11. Right to Alter Quantities

The Bank reserves the right to alter the requirement specified in the RFP. The Bank also reserves the right to delete one or more items from scope of Services specified in the RFP.

11.12. No Commitment to Accept Lowest or Any Offer

11.12.1. The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.

11.12.2. The Bank will not be obliged to meet and have discussions with any ITSM Service Provider and/ or to entertain any representations in this regard.

11.12.3. The Bids received and accepted will be evaluated by the Bank to ascertain the best and lowest Bid in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all Bids at any point of time prior to the order without assigning any reasons whatsoever. The Bank reserves the right to float the RFP again.

11.13. Information Security

ITSM Service Provider will provide an undertaking to comply with the provisions of the Information Security Policy of the Bank, which shall be be provided to the successful ITSM Service Provider.

11.14. Assignment and Change of Control

11.14.1. Subject to Clause 11.4, the ITSM Service Provider shall not assign, transfer, delegate, or pledge any of its rights or obligations hereunder to any third party without the prior written consent of NABARD, provided that ITSM Service Provider shall ensure that any and all obligations shall be performed by such assignee in accordance with the terms herein and that the assignee complies with all rights, duties and obligations herein. NABARD shall be entitled to transfer and/ or assign the whole or any part of its respective rights and obligations hereunder to any third party.

11.14.2. At any point in time, in the event of change in ownership structure or change in control, in any manner whatsoever of the ITSM Service Provider, or if any person / entity that, as of the date of furnishing of response to the RFP by the ITSM Service Provider, does not possess, directly or indirectly, the power to direct or cause the direction of the management, policies or affairs of the ITSM Service Provider, whether through the ownership of voting securities, by contract or otherwise, later comes into possession of such power, ITSM Service Provider shall inform NABARD in writing of such change in control along with the details of new ownership structure or persons / entities in control. In such event NABARD shall have the right to terminate the Contract/reject the Bid with/of the selected ITSM Service Provider and invoke the bid/performance security.

11.15. No Employer – Employee Relationship

The Contract shall be on a principal to principal basis and nothing in this RFP or the Contract (or any other arrangements contemplated herein) shall be deemed to create any employment or constitute a partnership or joint venture between the Parties or any of their holding / subsidiary / joint-venture / affiliate / group / client companies or any of their employees / officers / staff / personnel / representatives / agents and shall not, except as may be expressly provided herein, constitute any Party as the agent or legal representative of another Party for any purpose, or entitle any Party to commit or bind another Party in any manner.

11.16. Business Continuity

The selected ITSM Service Provider agrees for the following continuity arrangements to ensure the business continuity of the Bank:

11.16.1. In the event of this agreement comes to end on account of termination or by the expiry of the term/renewed term of the agreement or otherwise, the ITSM Service Provider shall render all technology and other reasonable assistance and help required by the Bank and to any new service provider engaged by the Bank, for a period of 180 (one hundred and eighty) days after the termination or expiry of the Contract for the smooth switch over and continuity of the Services. ITSM Service Provider agrees to provide all relevant documentation, and transitional support in respect of the Services and other matters to any new service provider engaged by the Bank to ensure that there are no interruptions or disruptions of any kind to NABARD's systems and operations.

11.16.2. In the event of failure of the ITSM Service Provider to render the Service, without prejudice to any other right, the Bank shall have as per this RFP and the Contract, the Bank at its sole discretion may make alternate arrangements for getting the Services from any other source. And if the Bank gives a prior notice to the ITSM Service Provider before availaing such service from any other alternative source, the ITSM Service Provider shall be liable to reimburse the expenses, if any incurred by the Bank in availing such services from the alternative source.

11.17. Co-operation

11.17.1. The ITSM Service Provider agrees to provide full co-operation and support to NABARD and / or its designee, at no additional cost, including by way of providing data, technology architecture and access to all non-proprietary/open source technology relating to the Comprehensive IT Services mangement, within such timelines as may be reasonably required by NABARD.

11.17.2. The ITSM Service Provider shall not commit any act or omission, whether directly or indirectly, to frustrate the intent of this Clause. Failure by the ITSM Service Provider to co-operate in the manner required by NABARD shall be deemed to be a breach of the Contract.

11.18. Intellectual Property Rights and Ownership

11.18.1. Parties acknowledge the Deliverables created by the selected ITSM Service Provider pursuant to the Contract are on "work-for-hire" basis. Accordingly, NABARD shall be the first owner of all Deliverables and all intellectual property rights with respect thereto. NABARD's ownership of the Deliverables will include all changes and additions to any Deliverables made by either Party and all derivative works created by either Party. To the extent that under Applicable Law, NABARD is not deemed to be the owner of the Deliverables, the selected ITSM Service Provider irrevocably agrees to assign, transfer and convey, without any reservations, all rights, title and interest in and to the Deliverables to NABARD, in all mediums, and modes now known or in future discovered, on a worldwide and perpetual basis, without further compensation other than the Contract Price.

11.19. Corrupt and fraudulent practice

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the execution of this RFP and subsequent contract(s). In this context, the ITSM Service Providers to note the following:

11.19.1. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

11.19.2. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among ITSM Service Providers (prior to or after Bid submission) designed to establish Bid prices at artificial non- competitive levels and to deprive the Bank of the benefits of free and open competition.

11.19.3. "Coercive practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any person or property to influence any person's participation or action in the bidding process;

11.19.4. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by the Bank with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the bidding process; or (ii) having a conflict of interest; and

11.19.5. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among ITSM Service Providers with the objective of restricting or manipulating a full and fair competition in the bidding process

11.19.6. The ITSM Service Providers and their respective officers, employees, agents and other representatives shall observe the highest standard of ethics during the bid process. Notwithstanding anything to the contrary contained in this RFP, the Bank reserves the right to reject a Bid and declare a ITSM Service Provider ineligible for a period of three years to be awarded any contract by NABARD, if at any time it determines that the ITSM Service Provider has engaged in any of the above practices in competing for or in executing a contract and shall be entitled to invoke any bid/performance bond/security as the case may be without prejudice to any other right or remedy that may be available to NABARD under this RFP or Applicable Law.

11.20. Waiver

11.20.1. To the extent permitted by Applicable Law: (a) no claim or right arising out of this RFP and/or the Contract or the documents referred to in this RPF can be discharged by one Party, in whole or in part, by a waiver or renunciation of the claim or right unless in writing signed by the Party or Parties giving the same; (b) no waiver that may be given by a Party will be applicable except in the specific instance for which it is given; and (c) no notice to or demand on one Party will be deemed to be a waiver of any obligation of such Party or of the right of the Party giving such notice or demand to take further action without notice or demand as provided in this RPF and/or the Contract or the documents referred to in this RPF.

11.20.2. The rights and remedies of the Parties hereto are cumulative and not alternative. Except where a specific period for action or inaction is provided herein, neither failure nor any delay on the part of either Party relating to the exercise of any right, power, privilege or remedy provided under this RFP or the Contract with the other Party shall operate as a waiver of such right, power, privilege or remedy or as a waiver of any preceding or succeeding breach by the other Party nor shall any single or partial exercise of any right, power, privilege or remedy preclude any other or further exercise of such or any other right, power, privilege or remedy provided in this RFP or the Contract, all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either Party at law or in equity. The failure of a Party to exercise any right conferred herein within the time required shall cause such right to terminate with respect to the transaction or circumstances giving rise to such right, but not to any such right arising as a result of any other transactions or circumstances.

11.21. Cumulative Remedy

Irreparable damage may occur if any of the provisions of this RPF and/or the Contract were not performed in accordance with their specific terms or otherwise; and therefore the Bank shall be entitled to seek an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the ITSM Service Provider from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. All rights, remedies or benefits provided for by Applicable Law or in this RFP and/or the Contract, and the exercise of any remedy by NABARD or the ITSM Service Provider shall not be deemed an election to the exclusion of any other remedy.

11.22. Confidentiality

11.22.1. All confidential information (from either party) is deemed as confidential within 15 days of disclosure by the disclosing party. This confidentiality restrictions shall be for the term of the resultant contract and for a period of two years thereafter. This restriction does not limit the right to use information contained in the data if it.

11.22.2. The ITSM Service Provider will be exposed by virtue of the contracted activities to the internal business information of Bank, affiliates, and/or business partners. Disclosures of receipt of this RFP or any part of the aforementioned information to Parties not directly involved in providing the Services requested could result in the disqualification of the ITSM Service Provider, premature termination of the Contract, or legal action against the ITSM Service Provider for breach of trust.

11.22.3. In case the selected ITSM Service Provider acts is extending similar services to multiple customers, ITSM Service Provider shall take care to build strong safeguards so that there is no co-mingling of information, documents, records and assets related to Services within the ambit of this RFP and subsequent purchase order.

11.22.4. The ITSM Service Provider shall not, without the written consent of the Bank, disclose the Contract or any provision thereof, any specification, or information furnished by or on behalf of the Bank in connection therewith, to any person(s).

11.22.5. Confidential Information shall not be used, reproduced or derived any benefit out of in any form except as required to accomplish the intent of this RFP. Any reproduction of any Confidential Information of NABARD shall remain the property of NABARD and shall contain any and all confidential or proprietary notices or legends which appear on the original. With respect to the Confidential Information of NABARD, the ITSM Service Provider (i) shall take all Reasonable Steps (defined below) to keep all Confidential Information strictly confidential; and (ii) shall not disclose any Confidential Information of the other to any person other than individuals such as counsel, directors, officers, employees, agents and representatives whose access is necessary to enable it to exercise its rights and/or perform its obligations hereunder and who are under obligations of confidentiality substantially similar to those set forth herein. As used herein “Reasonable Steps” means those steps the ITSM Service Provider takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care. If the ITSM Service Provider is compelled by Applicable Law or legal process to disclose Confidential Information of NABARD, it shall provide NABARD with prompt prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at NABARD’s expense, if NABARD wishes to contest the disclosure.

11.22.6. The ITSM Service Provider shall not, without the prior written consent of the Bank, make use of any document or information except for purposes of performing its obligations hereunder .

11.22.7. The above restrictions on the use or disclosure of the Confidential Information shall not apply to any Confidential Information that: (i) as evidenced in writing, is independently developed by the recipient without reference to the discloser’s Confidential Information and without breaching confidentiality obligations, or is lawfully received free of restriction from a third party having the right to furnish such Confidential Information; (ii) is or has become generally available to the public without breach of this RFP by the recipient; (iii) as evidenced in writing, at the time of disclosure, was known to the recipient free of restriction and was not unlawfully appropriated; or (iv) the discloser agrees in writing is free of such restrictions.

11.22.8. The selected ITSM Service Provider shall submit a non-disclosure agreement as per Annexure -XIII on non-judicial stamp paper of appropriate value.

11.22.9. The ITSM Service Provider shall not publish or disclose in any manner, without the Bank’s prior written consent, the details of any security safeguards designed, developed or implemented by the ITSM Service

Provider under the Contract or existing at any Bank location. The ITSM Service Provider shall develop procedures and implementation plans to ensure that IT resources leaving the control of the Bank (removed for repair, replaced or upgraded) are cleared of all Bank data and software. The ITSM Service Provider shall also ensure that all subcontractors (if permitted in Contract) who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed or implemented by the ITSM Service Provider under this RFP or the Contract or existing at any Bank location.

11.22.10. Upon request of NABARD, the ITSM Service Provider shall promptly and shall ensure that their Affiliates, directors, officers, agents, counsel, representatives and employees promptly: (i) return all documents containing Confidential Information, and (ii) destroy any copies of such documents, and any documents or other records (whether written or electronic) other than Confidential Information that may have been stored electronically as part of routine data back-ups which cannot be destroyed, to which these confidentiality obligations will continue to apply, and which should be kept strictly confidential by taking Reasonable Steps.

11.23. Service Level Agreement

The selected ITSM Service Provider shall execute a Service Level Agreement (SLA) with the Bank based on the terms tentatively set out under Annexure-XVI on a non-judicial stamp paper of appropriate value. The final form of the SLA shall be as determined by NABARD at the time of the execution of the Contract.

11.24. IPR Infringement

11.24.1. In the event of any claim of infringement of intellectual property rights arising from use of the Comprehensive IT Services mangement or any component thereof by the NABARD, NABARD may, at its option require the ITSM Service Provider to: (i) obtain the right to permit NABARD to continue using the Comprehensive IT Services mangement or the relevant component therof, or (ii) modify or replace the relevant portion(s) of the Comprehensive IT Services mangement with a non-infringing alternative having substantially equivalent performance within a reasonable period of time.

11.24.2. NABARD's rights set out herein shall not prejudice any other remedy available to NABARD under the Contract including but not limited indemnity or the right to terminate the Contract.

11.24.3. As a condition to avail the foregoing indemnity, the NABARD agrees to notify ITSM Service Provider in writing of the claim; and allow the ITSM Service Provider to control, and cooperates with the NABARD in, the defense and any related settlement negotiations.

11.24.4. ITSM Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) ITSM Service Provider's compliance with Bank's specific technical designs or instructions (except where ITSM Service Provider knew or should have known that such compliance was likely to result in an infringement claim and NABARD did not inform NABARD of the same); (ii) inclusion in a deliverable of any content or other materials provided by NABARD and the infringement relates to or arises from such NABARD materials or provided material; (iii) modification of a deliverable after delivery by ITSM Service Provider to NABARD if such modification was not made by or on behalf of ITSM Service Provider; (iv) operation or use of some or all of the deliverable in combination with products, information, specification, instructions, data, materials not provided by ITSM Service Provider; or (v) use of the deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable statement of work by ITSM Service Provider; or (v) use of a superseded release of some or all of the deliverables or NABARD's failure to use any modification of the deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by ITSM Service Provider.

11.25. Limitation of Liability

ITSM Service Provider's aggregate liability under the Contract shall be limited to a maximum of an amount equivalent to 100% of the Contract Price.

This limitation shall not apply to claims for:

1. infringement of third party intellecutal property, or breach of confidentiality;
2. gross negligence, wilful misconduct or any criminal liability.

Neither Party shall be liable for any indirect, consequential, incidental or special damages under the Contract.

Neither Party shall be liable for any indirect, consequential, incidental, consequential, punitive or special damages under the Contract, even if such party has been advised of the possibility of such damages.

ITSM Service Provider shall be excused and not be liable or responsible for any delay or failure to perform the services or failure of the services or a deliverable under this Agreement, to the extent that such delay or failure has arisen as a result of any delay or failure by the NABARD or its employees or agents or third party service providers to perform any of its duties and obligations as set out in this Agreement. In the event that ITSM Service Provider is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the NABARD, then ITSM Service Provider shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which ITSM Service Provider is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the NABARD. Such failures or delays shall be brought to the notice of the NABARD and subject to mutual agreement with the NABARD, then ITSM Service Provider shall take such actions as may be necessary to correct or remedy the failures or delays. ITSM

Service Provider shall be entitled to invoice the NABARD for additional costs incurred in connection with correction or remedy as above at time & material rate card as agreed upon between the parties.

11.26. Audit

11.26.1. NABARD would require the independent right to conduct its own audit, specifically with regard to the hardware and software used to provide services under the contract, by the ITSM Service Provider. The selected ITSM Service Provider shall allow the Bank, its authorised personnel, its auditors (internal and external), authorised personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the Services. In case any of the Services are further outsourced/assigned/ subcontracted to other ITSM Service Providers, it will be the responsibility of the ITSM Service Provider to ensure that the authorities / officials as mentioned above are allowed access to all the related places, for inspection and verification.

The audit requirement under this sub-clause is in relation to the RBI / regulatory authorities and cannot be subject to prior permission.

11.26.2. The selected ITSM Service Provider shall, whenever required by such auditors, furnish all relevant information, records/data to them. The ITSM Service Provider shall bear the cost of one audit per year by NABARD. If NABARD undertakes any subsequent audits in a relevant year, then the cost for such audits shall be borne by NABARD. NABARD may conduct an audit or inspection by providing the selected ITSM Service Provider at least 7 (seven) Business Days' prior written notice, however prior notice may not be given for audit or inspection conducted by regulatory authority.

11.26.3. Where any deficiency has been observed during audit of the selected ITSM Service Provider on the risk parameters finalized by the NABARD or in the certification submitted by the auditors, it is agreed upon by the ITSM Service Provider that it shall correct/ resolve the same, within timelines prescribed by NABARD. In such instance, any cost incurred by NABARD in undertaking the audit, shall be reimbursed by the ITSM Service Provider to NABARD immediately, and in no event later than 7 (seven) days from completion of audit report. The ITSM Service Provider shall provide certification of the auditor to the NABARD regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed.

11.26.4. NABARD reserves the right to call for and/or retain any relevant material information / reports including audit or review reports undertaken by the ITSM Service Provider (e.g., financial, internal control and security reviews) and findings made on the ITSM Service Provider in conjunction with the Services provided to the NABARD.

11.26.5. The ITSM Service Provider shall also get itself audited by internal or external empaneled auditors appointed by NABARD, on an annual basis, covering the risk parameters finalized by NABARD such as IT hardware, software, data privacy, cybersecurity, regulatory or statutory compliance. The ITSM Service Provider shall submit the certification received by it from the relevant auditors to NABARD. The ITSM Service Provider shall permit any audit by inspecting officials from the Reserve Bank of India or any regulatory authority as required under Applicable Law.The ITSM Service Provider and/ or its permitted sub – contractors shall facilitate any audit required pursuant to this Clause.

11.27. Right of Publicity

Any publicity by the ITSM Service Provider in which the name of NABARD is to be used should be done only with the explicit written permission of NABARD.

11.28. Indemnity

11.28.1. The ITSM Service Provider assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of (i)any breach of the ITSM Service Provider's obligation under these general conditions or (ii) for which the ITSM Service Provider has assumed responsibilities under the Contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the ITSM Service Provider in connection with the performance of any system covered by the Contract or (iii) acts or omissions of the ITSM Service Provider which amount o negligence or wilful misconduct; or (iv) any losses arising out of or in relation to any accident or injury sustained or suffered by the ITSM Service Provider's workmen, contractors, sub- contractors, service providers, agent(s), employed/ engaged otherwise working for the ITSM Service Provider or by any other third party resulting from or by any action, omission, or operation conducted by or on behalf of the ITSM Service Provider. The ITSM Service Provider shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the Contract and to protect the Bank during the tenure of purchase order.

11.28.2. Where any patent, trade mark, registered design, copyrights and/ or intellectual property rights vest in a third party or in the event of any infringement of alleged infrongement by ITSM Service Provider of third party's intellectual property or NABARD's intellectual property, the ITSM Service Provider shall be liable for settling with and paying any license fee, royalty and/ or compensation thereon.

11.28.3. The rights of NABARD pursuant to this Clause 11.29 shall be in addition to and not exclusive of, and shall be without prejudice to, any other rights and remedies available to NABARD at equity or law including the right to seek specific performance, rescission, restitution or other injunctive relief, none of which rights or remedies shall be affected or diminished thereby.

11.28.4. Indemnification Procedure for Third-Party Claims

(i) In the event that NABARD receives notice of the assertion of any claim or the commencement of any action by a third-party in respect of which indemnity may be sought under the provisions of this Clause 11.29 (a "**Third-Party Claim**"), NABARD shall notify ITSM Service Provider in writing of such Third-Party Claim (such notice, a "**Notice of Claim**") within 10 (ten Business Days of receipt of notice thereof; provided that the failure or delay in notifying the ITSM Service Provider of such Third-Party Claim will not relieve the ITSM Service Provider of any liability it may have towards NABARD.

(ii) The ITSM Service Provider shall assume the defense or prosecution of such Third-Party Claim and any litigation resulting therefrom with counsel acceptable to NABARD and at the sole cost and expense of the ITSM Service Provider (a "**Third-Party Defense"**). The ITSM Service Provider shall undertake the investigation, defense and settlement thereof in agreement with NABARD. The ITSM Service Provider will not consent to the entry of any judgment or enter into any settlement with respect to the Third-Party Claim without the prior written consent of NABARD. NABARD may retain separate co-counsel at the expense of the ITSM Service Provider. Upon assumption of the defense of a Third Party Claim, the ITSM Service Provider shall be conclusively deemed to have acknowledged that the Third-Party Claim is within the scope of its indemnity obligation under this Contract. The ITSM Service Provider shall conduct the Third-Party Defense actively and diligently and provide copies of all correspondence and related documentation in connection with the Third-Party Defense to NABARD to the extent it does not adversely affect attorney-client privilege. The ITSM Service Provider will not take any action, or omit to take any action, without the consent of NABARD, that would cause (x) any contracts, correspondence or other documents or confidential information of NABARD or its affiliates to be disclosed to a third-party or (y) any director, officer, employee or agent of NABARD to take any action related to the Third-Party Claim which could reasonably be expected to interfere with or contravene such person's duties to NABARD or its affiliates. NABARD will provide reasonable cooperation in the Third-Party Defense.

(iii) Notwithstanding the foregoing, ITSM Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) ITSM Service Provider's compliance with NABARD's specific technical designs or instructions (except where ITSM Service Provider knew or should have known that such compliance was likely to result in an infringement claim and NABARD did not inform ITSM Service Provider of the same); (ii) inclusion in a deliverable of any content or other materials provided by NABARD and the infringement relates to or arises from such NABARD materials or provided material; (iii) modification of a deliverable after delivery by ITSM Service Provider to NABARD if such modification was not made by or on behalf of ITSM Service Provider;

(iv) operation or use of some or all of the deliverable in combination with products, information, specification, instructions, data, materials not provided by ITSM Service Provider; or (v) use of the deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable statement of work by ITSM Service Provider; or (v) use of a superseded release of some or all of the deliverables or NABARD's failure to use any modification of the deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by ITSM Service Provider.

(iv) If counsel for NABARD reasonably determines that there are legal defenses available to NABARD different from or in addition to those available to the ITSM Service Provider or an actual conflict of interest exists between NABARD and the ITSM Service Provider in the defense of any Third-Party Claim, then counsel for NABARD shall be entitled, if NABARD so elects, to conduct the defense to the extent reasonably determined by such counsel to protect the interests of NABARD, at the expense of the ITSM Service Provider.

(v) If the ITSM Service Provider does not assume the Third-Party Defense, NABARD shall have the right to assume the Third-Party Defense with counsel of its choice at the expense of the ITSM Service Provider; provided, that NABARD shall control the investigation, defense and settlement thereof. NABARD shall have the right to agree to the entry of any judgment or enter into any settlement with respect to the Third-Party Claim.

(vi) The ITSM Service Provider will not be entitled to assume the Third-Party Defense if: (i) the Third-Party Claim seeks, in addition to or in lieu of monetary damages, any injunctive or other equitable relief, other than injunctions seeking to terminate or limit the Services; (ii) the Third-Party Claim relates to or arises in connection with any criminal action, indictment or allegation; (iii) NABARD reasonably believes an adverse determination with respect to the Third-Party Claim would be detrimental to or injure NABARD's reputation or business prospects; (iv) ITSM Service Provider has failed or is failing to vigorously prosecute or defend such Third-Party Claim (as reasonably determined by NABARD); or (vi) the ITSM Service Provider fails to provide reasonable assurance to NABARD of its financial capacity to prosecute the Third-Party Defense. In such instance, NABARD shall have the right to assume the Third-Party Defense with counsel of its choice at the expense of the ITSM Service Provider; and NABARD shall control the investigation, defense and settlement thereof. NABARD shall have the right to agree to the entry of any judgment or enter into any settlement with respect to the Third-Party Claim.

(vii) It is further clarified that NABARD would require the detailed indemnity clause set out in Clauses 11.29.1 -11.29.4 contract as it specifically sets out the independent agreement between the parties on the rights that may be availed by NABARD against the ITSM Service Provider in the instance of breach of any obligations of the ITSM Service Provider or any claims arising against NABARD due to certain acts / omissions of the ITSM Service Provider. Indemnity is in addition to and separate from other contractual remedies available to the parties.

11.29. Force majeure

11.29.1. If the performance as specified in this Contract is prevented, restricted, delayed or interfered with for any cause beyond the control of the Parties, including by reason of fire, explosion, cyclone, floods, war, hostilities, revolution, riots, acts of public enemies, espionage, blockage or embargo, pandemic, epidemic, lockdowns, acts of God, network failure or failure of electronic transmission, default or failure of/by any third party, any law, order, proclamation, ordinance, demand or requirements of any Government or authority or representative of any such Government including restrictive trade practices or regulations, strikes, lockouts, shutdowns or labour disputes which are not instigated for the purpose of avoiding obligations herein, or any other circumstances beyond the control of the Party affected, provided that the current ongoing situation regarding COVID-19 and/or lockdowns due to COVID-19 shall not be considered a force majeure event under this Contract (**"Force Majeure Event"**), then notwithstanding anything here before contained, the Party affected shall not be considered to be in default of performance of obligations under the terms of this Contract or for indemnification provided for hereunder to the extent such performance relates to prevention, restriction, delay or interference. and provided the Party so affected uses its best efforts to remove such cause of non-performance and when removed the Party shall continue performance with utmost dispatch.

11.29.2. If a Force Majeure Event arises, the ITSM Service Provider shall promptly notify the Bank in writing of such condition, the cause thereof and the change that is necessitated due to the conditions. Until and unless otherwise directed by the Bank in writing, the ITSM Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure Event. If NABARD determines it is commercially or technically infeasible to cure the Force Majeure Event and so notifies the ITSM Service Provider , then NABARD may terminate the Contract effective immediately upon delivery of notice of termination to the ITSM Service Provider

As there is dependency of NABARD solely on the ITSM Service Provider for the performance of services, if NABARD determines that it is not commercially or technically feasible for the ITSM Service Provider to provide the services due to a force majeure event, it should be entitled to terminate the agreement immediately. Separately the clause also provides that the ITSM Service Provider would not be held to be in default of its obligations or liable to provide indemnity for any failure to perform due to a force majeure event which should give the ITSM Service Provider additional comfort.

The Force Majeure clause contemplates that both parties may be affected by a Force Majeure Event and to that extent, the force majeure clause is mutual. Only the right of termination due to the occurrence of a force majeure event is restricted to NABARD owing to the fact that NABARD is the recipient of the service.

Given that force majeure events are not foreseeable, it is difficult to contemplate a specific timeline within which termination rights shall be made available to the Parties. However, it is clarified that to the extent the force majeure event affects the ITSM Service Provider, the ITSM Service Provider shall not be liable for delays caused due to such force majeure event.

11.30. Resolution of Disputes

11.30.1. All disputes and differences of any kind whatsoever, arising out of or in connection with this Contract or in the discharge of any obligation arising under this Contract (Whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Contract) shall be first resolved amicably by Parties. For the purpose of such amicable settlement, each Party shall within 7 days from the date either party notifies the other of a dispute having arisen, select / appoint 1 (one) senior representative from their respective management who shall undertake all discussions on behalf of their respective organisation, in order to settle the dispute amicably. Such discussions towards amicable settlement of the dispute shall be undertaken for a period of 30 days from the date of appointment of both the respective senior representatives ("**Settlement Period**").

11.30.2. In case of failure to resolve the disputes and differences amicably in accordance with Clause 11.31.1 prior to expiry of the Settlement Period, such unsettled dispute or difference shall be referred to and finally resolved by arbitration administered by the Mumbai Centre for International Arbitration in accordance with the Arbitration Rules of the Mumbai Centre for International Arbitration ("**MCIA Rules**") for the time being in force, which rules are deemed to be incorporated by reference in this Clause 11.31.

11.30.3. In the event of such arbitration:

(i) The language of the proceedings shall be in English;

(ii) the tribunal shall consist of 3 (three) arbitrators; 1 (one) to be appointed by NABARD, 1 (one) to be appointed by the ITSM Service Provider, and the third to be appointed by the 2 (two) arbitrators. If either NABARD or the ITSM Service Provider fails to appoint an arbitrator as set out in this Clause 11.31, the arbitrator of such Party shall be appointed in accordance with the MCIA Rules;

(iii) the tribunal shall be entitled to decide on and apportion the costs and reasonable expenses (including reasonable fees of counsel retained by the Parties) incurred in the arbitration;

(iv) the existence and content of any arbitration proceeding, and any award thereof shall be confidential among the Parties, and subject to the terms of Clause 11.22 hereof; and

(v) the existence or subsistence of a dispute between the Parties, or the commencement or continuation of arbitration proceedings, shall not, in any manner, prevent or postpone the performance of those obligations of

Parties under the Contract which are not in dispute, and the arbitrators shall give due consideration to such performance, if any, in making a final award.

11.30.4. The seat & venue of arbitration shall be in Mumbai. The award of the arbitrators shall be final and binding on the Parties and may be specifically enforced by any court of competent jurisdiction. It is hereby agreed that in all disputes referred to the arbitration, the arbitrators shall give a separate award in respect of each dispute or difference in accordance with the terms of reference and the award shall be a reasoned award. It is hereby agreed that the arbitrators shall not have powers to order any interim measures whatsoever during the course of arbitration.

11.30.5. Notwithstanding anything in the contrary set forth in this RFP, each Party shall be entitled to seek urgent interim relief in any court of competent jurisdiction, including pre-arbitral attachments, temporary restraining orders, or temporary injunctions, as may be necessary to preserve the rights of such Party. The application by either Party to a judicial authority for such measures shall not be deemed to be an infringement or a waiver of the covenant of the Parties to submit disputes to arbitration under this Contract and shall not affect the relevant powers reserved to the arbitrators pursuant to this Clause 11.31.

11.30.6. All disputes arising out of or in any way connected with this Contract shall be deemed to have arisen at Mumbai only and Courts in Mumbai only shall have jurisdiction to determine the same.

11.30.7. Any notice given by one Party to the other pursuant to the Contract shall be sent to the other Party in writing, by hand, registered post or email to the other Party's specified address. A notice shall be deemed delivered (i) if delivered by hand, upon delivery;(ii) if delivered by registered post, at the start of the second Business Day after the date of posting; or (iii) if delivered by email, when the sending of the email is recorded on the sender's computer unless the sender recieves a message indicating unsuccesful transmission.

11.30.8. For the purpose of all notices, the following shall be the address of NABARD:

The Chief General Manager
National Bank for Agriculture and Rural Development
Department of Information Technology,
C-24, 'G' Block,
Bandra Kurla Complex
Bandra (East), **Mumbai 400 051**
Email:dit@nabard.org

11.30.9. Notices to the ITSM Service Provider shall be sent to the registered address of the ITSM Service Provider and email ID as provided by the ITSM Service Provider under the Contract / in response to this RFP.

11.31. Other Clauses

11.31.1. NABARD has the sole ownership of and the right to use, all data that may be in possession of the ITSM Service Provider or its representative in the course of performing the Services under the agreement that may be entered into. All documents, reports, information, data etc. collected and prepared by ITSM Service Provider in connection with the Scope of Work submitted to NABARD will be property of the Bank. The ITSM Service Provider shall not be entitled either directly or indirectly to make use of the documents, reports given by NABARD for carrying out of any Services with any third parties. ITSM Service Provider shall not without the prior written consent of NABARD be entitled to publish studies or description article with or without illustrations or data in respect of or in connection with the performance of Services.

11.31.2. No provision of the RFP is intended to, or shall, confer any right on a third-party beneficiary or other rights or remedies upon any person other than the Parties hereto; nor impose any obligations on the part of the Parties to the agreement towards any third parties.

11.31.3. The ITSM Service Provider shall be entirely responsible for all applicable taxes, duties, levies, charges, license fees, road permits, etc., in connection with delivery of products/Services at site including incidental Services and commissioning.

11.31.4. The ITSM Service Provider should also ensure that all Applicable Laws framed by the Central Government, State Government and Local bodies, including payment of applicable minimum wages and all laws pertaining to contract employees/labour laws are complied with while providing caretaker services. The selected ITSM Service Provider may have to execute an indemnity bond in favour of the Bank in this regard.

It is a specific obligation for the ITSM Service Provider to comply with applicable laws while providing the Services and NABARD may be exposed to liability for any breach of applicable law by the ITSM Service Provider, NABARD would require a specific indemnity bond with regard to such compliances independent of the contract.

11.31.5. Providing clarifications / particulars / documents, etc., to the appropriate tax authorities for assessment of tax, compliance with labour and other laws, etc will be the responsibility of the ITSM Service Provider at his cost.

11.31.6. Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall affect such deductions from the payment due to the ITSM Service Provider. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the ITSM Service Provider from his responsibility to pay any tax that may be levied in India on Income and Profits made by the ITSM Service Provider in respect of this Contract.

11.32. Representation and Warranties

The selected ITSM Service Provider shall be deemed to have made the following representations and warranties as of the date of the Bid:

11.32.1. That the selected ITSM Service Provider has the requisite qualifications, skills experience and expertise in providing Services contemplated hereunder. It has the technical know-how and the financial wherewithal, the power and the authority to enter into the Contract and provide the Service / Systems sought to NABARD and shall undertake all Services and obligations under this Contract on a first priority basis.

11.32.2. That the selected ITSM Service Provider is not involved in any litigation, potential, threatened / existing that may have an impact of affecting or compromising the performance and delivery of Services / Systems under the Contract.

11.32.3. That the selected ITSM Service Provider is not bankrupt or insolvent under the Applicable Laws of its applicable jurisdiction and there are no insolvency proceedings of any character, including without limitation, bankruptcy, receivership, reorganization, composition or arrangement with creditors, voluntary or involuntary, affecting it, or is pending or, to the best of its knowledge, threatened in writing, and it has not made any assignment for the benefit of creditors or taken any action in contemplation of, or which would constitute the basis for, the institution of such insolvency proceedings.

11.32.4. That the representations made by the selected ITSM Service Provider in its Bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the Contract and the Bid Documents and unless NABARD in writing specifies to the contrary, the selected ITSM Service Provider shall be bound by all the terms of the Bid.

11.32.5. That the selected ITSM Service Provider has professional skills, personnel and resources / authorisation that are necessary for providing all such Services as are necessary to perform its obligations under the Bid and this Contract.

11.32.6. That the selected ITSM Service Provider shall ensure that all assets including but not limited to software’s, licenses, databases, documents etc. developed, procured, deployed and created during the terms of the Contract are duly maintained and suitably updated, upgraded, replaced with regard to contemporary and statutory requirements.

11.32.7. That the selected ITSM Service Provider shall use assets as NABARD may permit for the sole purpose of execution of its obligations under the terms of the Bid, RFP or the Contract. The selected ITSM Service Provider shall, however, have no claim to any right, title, lien or other interest in any such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.

11.32.8. That the selected ITSM Service Provider shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted process / product free from all claims, titles, interests and liens thereon and shall keep NABARD, its directors, officers, employees, representatives, consultant and agents indemnified in relation thereto.

11.32.9. That all the representations and warranties as have been made by the selected ITSM Service Provider with respect to its Bid and Contract, are true and correct, and shall continue to remain true and correct through the term of the Contract.

11.32.10. That the execution of the Services would be in accordance and in compliance with all Applicable Laws as amended from time to time and the regulatory framework governing the same.

11.32.11. That there are no inquiries or investigations have been threatened, commenced or pending against the selected ITSM Service Provider or its team members by and statutory or regulatory or investigative agencies.

11.32.12. That the selected ITSM Service Provider has the corporate power to execute, deliver and perform the terms and provisions of the Contract and has taken all necessary corporate action to authorise execution, delivery and performance by it of the Contract.

11.32.13. That neither the execution and delivery by the selected ITSM Service Provider of the Contract nor the selected ITSM Service Provider's compliance with or performance of the terms and provisions of the Contract will contravene any provision of any Applicable Law or any order, writ, injunction or decree of any court or Governmental authority binding on the selected ITSM Service Provider nor will it conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the selected ITSM Service Provider is a Party or by which it or any of the property or assets is bound or to which it may be subject or violate any provision of the constitution documents of the selected ITSM Service Provider.

11.32.14. That the selected ITSM Service Provider certifies that all registrations, recording, filings and notarizations of the Contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the selected ITSM Service Provider which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been made.

11.32.15. That there has not and shall not occur any execution, amendment or modification of any Contract without the prior written consent of NABARD, which may directly or indirectly have a bearing on the Contract or Services rendered.

11.32.16. That no sums, in cash or kind, have been paid or shall be paid, by the selected ITSM Service Provider or on its behalf, to any person by way of fees, commission or otherwise for entering into the Contract or for influencing or attempting to influence any officer or employee of NABARD in connection therewith.

11.32.17. The selected ITSM Service Provider shall not, make any announcements or statements to any person that are or may be derogatory, defamatory or prejudicial to NABARD, or any of its affiliates, directors, employees, officers, agents or advisors, in any manner.

11.32.18. Appropriately qualified personnel appointed by the selected ITSM Service Provider shall perform Services with due care and diligence and to such high standards of quality as it is reasonable for NABARD to expect in all the circumstances post the expiry of this Contract.

11.32.19. The selected ITSM Service Provider further undertakes to exercise all due diligence with regard to and shall maintain strict controls and physical and digital safeguards in connection with the Services.

11.32.20. That no representation or warranty by it contained herein or in any other document furnished by the selected ITSM Service Provider to NABARD or to any government instrumentality in relation to the Services contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading.

11.32.21. That the selected ITSM Service Provider shall ensure that the employees of the ITSM Service Provider/ third party sub-contractors who are engaged in providing the Services under this Contract shall have executed/ execute such confidentiality documents as may be required by NABARD and shall have confidentiality obligations not lesser than those prescribed under this Contract.

Confidentiality contracts with employees will only be held to be compliant with the terms of the agreement so long as they provide terms which are no less severe than the terms mentioned in the RFP.

11.32.22. The selected ITSM Service Provider shall be fully and completely responsible and liable for all acts, omissions, liabilities undertaken by personnel employed / engaged by the selected ITSM Service Provider and shall be solely responsible for any and all claims, payments and benefits payable to such personnel employed by the ITSM Service Provider.

11.32.23. The selected ITSM Service Provider will not violate the intellectual property rights of third parties whilst providing the Services.

11.32.24. The selected ITSM Service Provider has adequate insurance, risk management systems, contingency plans and backup system in place to ensure that it may continue to provide uninterrupted performance of Services consistent with the standards agreed herein.

11.32.25. The selected ITSM Service Provider agrees that NABARD shall retain real and effective control / retention of full ownership of the Deliverables and Comprehensive IT Services mangement at all times during and after the term of the RFP and Contract.

****

1. Annexure I – Bid Forwarding Letter

(To be submitted on Bidder's Letter Head)

Date:

The Chief General Manager
Department of Information Technology
National Bank for Agriculture and Rural Development,
5th Floor, C-24, G Block
Bandra Kurla Complex (BKC), Bandra (E)
Mumbai - 400 051

Dear Sir,

Comprehensive IT Services Management for NABARD

We, the undersigned, offer to submit our Bid in response and accordance with your tender No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022 having examined the tender document including all Annexures carefully, we are hereby submitting our proposal along with all the requisite EMD and other documents as desired by the Bank.

If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this Bid together with your written acceptance thereof shall constitute a binding contract between us.

Further, we agree to abide by all the terms and conditions as mentioned herein in the tender document.

We agree to abide by this offer till 180 days from the date of last day for submission of offer (Bid).

We agree that, the rates quoted by us would serve as a rate contract for future additional services.

We agree that, the Bank will pay power charges based on actual power units consumed.

We hereby agree to participate and abide by the methods of evaluation indicated in the RFP.

We have also noted that NABARD reserves the right to consider/ reject any or all Bids without assigning any reason thereof.

We understand that the Bank is not bound to accept any proposal it receives.

Dated at _______ day of ________ 2022.

Yours sincerely,

Date **Signature of Authorised Signatory:**

Place **Name of the Authorised Signatory:**

Designation:

Phone & E-mail:

Name of the Organisation:

Seal

2. Annexure II : Details of Bidder

S. N.		**Documents to be Submitted**	**ITSM Service Provider's Response** (to be filled in by ITSM Service Provider)
1	Name of the Bidder		
2	Year of establishment		
3	Ownership Bidder		
4	Registration number and date of registration.	*Copy of Registration Certificate.*	
5	Registered Office Address.		
6	GST Number	*Copy of GST Registration certificate*	
7	PAN No.	*Copy of PAN number.*	
8	**Promotor / Director Details**		
a	Name		
b	Designation (Promoter / Director)		
c	Mobile No.		
d	Mail Id		
9	***Address of Bidder Office at Mumbai with contact numbers***		
a	Address		
b	Land Line No.		
c	Mail Id.		
10	**Contact Details of Bidders authorized Representative (on whose behalf Power of Attorney issued).**		
a	Name		
b	Designation		
c	Mobile No.		
d	Mail id		
e	Specimen Full Signature and initials.		
11	**MSME Details**		
A	Whether Bidder MSME (Yes/No)		
B	MSME Registration No		

S. N.		Documents to be Submitted	ITSM Service Provider's Response (to be filled in by ITSM Service Provider)
C	Date till which MSME Certificate is valid.		
D	Attested Copy of MSME Certificate attached. (Yes /No)		
12	**Bank Account Details**		
A	Bank Name		
B	Account Number		
C	IFSC Code		
D	Account Type		
E	Copy of Cancelled Cheque attached. (Yes /no)		
F	Bank Mandate form as per **Annexure–XI** attached. (Yes/No).		

I certify that the above-mentioned information and the relevant annexure and enclosures are true and correct.

Date:
Place:

Name of the Authorized Signatory
Designation

Name of Organisation

Seal

Note

1. Bidder response should be complete with all relevant documents attached.
2. Documentary proof, sealed and signed by authorized signatory, should be submitted
3. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. NABARD will not make any separate request for submission of such information.
4. NABARD will contact the Bidder referenced customer for verifications of facts and, the Bidder may ensure that the customer is intimated in this regard. Further in case NABARD feels to visit the reference customer, the Bidder to take necessary approvals for the same. NABARD will not make any separate request to the Bidder's customers.

5. Proposal of the Bidders are liable to be rejected in case of incomplete information or non-submission of documentary proof.

3. ANNEXURE III : Minimum Eligibility Criteria

S.N.	Evaluation	Documents to be submitted	Compliance (Y/N)	Description of proof attached
1.	**Credentials** The Bidder should be a company incorporated under Companies Act 1956/2013 and having its registered office in India and dealing with IT related Services for at least 3 years immediately preceding the Bid submission	• Certificate of Registration issued by Registrar of Companies; • The latest registered copy of Memorandum and Articles of Association; • GST Registration Certificate; • Certificate from authorized signatory/ Company Secretary of the Bidder indicating that they are in IT Solution for last 3 years		
2.	**Financials** The Bidder should have a minimum annual turnover of Rs.500.00 crore and should also be in operating profit during the last three financial years, viz., 2018-19, 2019-20 & 2020-21 The Net worth of the Bidder should be positive as on 31 March 2021	• Audit Balance Sheets of last three FY viz. 2018-19, 2019-20 & 2020-21. • CA Certificate exclusively indicating the turnover, profit after tax for the last 3 years, and Net worth as on 31 March 2021		
3.	**Experience** The Bidder should have provided or is providing ITSM solution in atleast 3 institutions in India of which one should be in BFSI / Regulatory institutions in India, anytime during last seven years (i.e. Since April 2014). References of top three projects atleast one of Rs.10 Cr or above (in terms of size	Copies of POs (with commercials masked, if required) and a Letter from the Customer confirming the successful implementation of the solution in their organisation should be submitted. The letter should indicate the Start and End date of services. Contact Details of SPoC from the three organisations should also be furnished.		

S.N.	Evaluation	Documents to be submitted	Compliance (Y/N)	Description of proof attached
	of the solution) of the Bidder should be submitted. Incase Bidder has signed Confidentiality Agreement with Customers, a Self-Declaration by Bidder with Masked PO may be submitted			
4.	**Non Blacklisting** The Bidder should not have been blacklisted by any Bank, Financial Institution, Govt.'s Bidder Black List earlier.	Bidder should submit a declaration to the effect as per the format provided in Annexure-VII. If this declaration is found to be false, the Bank shall have the right to reject Bidder's offer and if the Bid has resulted in a contract, the contract is liable to be terminated		
5.	**Geographical Presence** Bidder should have its offices in at least 10 State Capitals in India. Specify locations and addresses along with details of office in charge. Submit List of offices with addresses signed by authorized signatory	Declaration from the authorized signatory along with the address, phone number and contact person of the location.		

4. ANNEXURE IV – Evaluation Methodology

4.1. Evaluation by the Technical Evaluation Committee

The Technical Bids would be evaluated by the Technical Evaluation Committee based on the technical evaluation criteria and sub criteria listed below

		Maximum Score	Weighted Maximum Score
Stage A (70% weight in Technical Score)	Compliance with Technical Requirements	100	70
Stage B (20% weight in Technical Score)	Presentation by Bidder and Demo of any tool proposed.	100	20
Stage C(10% in weight in Technical Score)	Minimum 3 reference of similar nature project and One Site visit preferably Mumbai	100	10

4.1.1. When deemed necessary the Tender Evaluation Committee may seek clarifications on relevant aspects from the Bidder. However, that would not entitle Bidder to change or cause any change

4.1.2. The scoring methodology for Technical Bid components is explained in the following paragraphs

4.1.3. Scores for the above individual parameters shall be added to determine the technical scores of the Bidders. The Bidder with the highest technical score shall be ranked as T1

4.2. Scoring Methodology for Stage A

4.2.1. The Bidder should provide a response to each of the requirements listed in Appendix VI. The response should specify whether the Comprehensive IT Services management proposed by the Bidder is compliant with the requirement or not. The compliance for each requirement should be marked as:

- Compliant Out-of-box
- Compliant with customization
- Non – Compliant

- The Bidder's response to the requirements stating how the Comprehensive IT Services management is compliant shall be evaluated. If the response has been filled against more than one head i.e. 'Compliant Out-of-box'', 'Compliant with customization', 'Non – Complaint', it shall be treated as 'Non-Compliant'. If any response is not filled, it shall be considered as 'Non-Compliant'

4.2.2. The functional and non-functional requirements mentioned in the Appendix VI are minimum requirements. The Bidder can suggest additional requirements as deemed necessary to cover the entire landscape of the proposed Comprehensive IT Services management. All costs associated with Out-of-box and customization of the Comprehensive IT Services management will be borne by the Bidder.

4.2.3. Scoring Methodology for Stage B

4.2.3.1. The Bidder should present proposed solution and its functionalities, plan of implementation, plan to manage day to day affairs of project.

4.2.3.2. Time slot of 30 minutes shall be allocated to each bidder for presentation.

4.2.3.3. Date & Time, place shall be intimated to eligible bidders later.

4.2.4. Scoring Methodology for Stage C.

4.2.4.1. Bidder shall provide reference 3 projects of similar nature with detailed implementation scope of work and implantation of projects.

4.2.4.2. Bidder shall provide one reference for site visit preferably in Mumbai

4.2.5. The technical requirements will be scored as below:

Functional Compliance	Evaluation	Score
Compliant as Out of Box functionality	Evaluated as 'Out of Box' functionality of the Comprehensive IT Services management	1
Compliant with customization	Evaluated as a functionality of the Comprehensive IT Services management with customization	0.75
Non compliance	Functionality is not available in the Comprehensive IT Services management	Technical bid will be rejected for any non-compliance

4.2.6. The Compliance Score A (based on response to technical requirements) is calculated as below:

$$A = \frac{(1 * \ No\ of\ compliant\ out\ of\ box + \ 0.75 * No\ of\ Complaint\ with\ Customization)}{Total\ Number\ of\ Technical\ Requirements}$$

4.2.5. Own Geographical Spread

Functional Compliance	Score
Physical office at NABARD office locations	1
Physical office at NABARD location is not present, however staff deputed for NABARD is on bidder payroll	0.75
Neither office at NABARD location is present, nor staff deputed for NABARD is on bidder payroll	0

D= ((1* Physical office at NABARD office locations + 0.75* Physical office at NABARD location is not present, however staff deputed for NABARD is on bidder payroll))/(Total Number of locations)

5. ANNEXURE V – Commercial Bid

FORMAT FOR FURNISHING AMC RATES

5.1. The format for Commercial Bid is given below. Bidder have to fill the fields concerned from the summary portion of the Annexure in the appropriate space given below;

5.1.1. The inventory list is only indicative – there may be deviations in the configurations, count and brand.

5.1.2. Bidder are requested to quote their best rate for each item, which are indicated in this Annexure.

5.1.3. All the costs should be exclusive of all taxes & levies, Break-up of taxes, levies, duties must be mentioned in separate table.

5.1.4. All licenses should be in name of NABARD.

QUOTE – A: This will have the rates of PCs, Laptops, Scanners, Printers and other items for the enclosed list of hardware for each location. **"Appendix IV"**

AMC details (For the complete IT Assets in the Bank including the list given in Appendix IV)

Office Location	Item	Amount				
		Year 1	Year 2	Year 3	Year 4	Year 5
1. Head Office	Desktop					
	AIO					
	Laptop					
	Printer					
	Scanner					
2. Regional Offices /Training Establishments	Desktop					
	AIO					
	Laptop					
	Printer					
	Scanner					
AMC Total (Figure I)						

Quote B:

Job Profile	Qty	Total Amount					
		Unit cost	Year 1	Year 2	Year 3	Year 4	Year 5
1. AMC for Computers and Peripherals + Desktop Management							
2. Patch Management + Data Center and							
3. Server Management							
3. Domain Services Management +File Services Management							
4. Network Management							
5. IT Security Management							
6. DBA(Oracle and MSSQL, MSSQL, Postgers)							
7. Vendor Management +Asset-Configuration-License Management							
8. Help/Service desk Management							
9. Patch Management +Data Center and Server Management							
10.AMC Engineer at each RO/TE							
FMS TOTAL (Figure II)							

As per Bank's understanding a total of 24 engineers with necessary skillsets as indicated the **Appendix III**. However, the bidder is expected to propose a suitable team structure, composition and number of engineer.

Quote C:

List of all Tools and Other Software Components (details) [Yearly Cost for individual software needs to be given]	Total Amount				
	Year 1	Year 2	Year 3	Year 4	Year 5
Tools Total (Figure III)					
Total Amount : Figure I + II + III (AMC + FMS+ Tools, etc)					

Quote D*:

Rate contract for DDMs office visit (Rate per visit for across all locations)	Total Amount				
	Year 1	Year 2	Year 3	Year 4	Year 5

***This is not part of the commercial bid for L1 calculation**

6. ANNEXURE VI – Letter of Authorisation to Bid

(To be executed on non-judicial stamp paper of Rs.500/-)

Ref No: ______________________ Date: --/--/2022

The Chief General Manager
Department of Information Technology,
National Bank for Agriculture and Rural Development
5th Floor, C Wing, C-24, 'G' Block, Bandra-
Kurla Complex, P.B. No. 8121, Bandra (East),
Mumbai - 400 051.
Maharashtra

Dear Sir,

Subject: Authorization Letter for submitting Bid documents.

REF: Your RFP No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022

This has reference to your above RFP for Comprehensive IT Services management for NABARD. Mr./Mrs./Miss______________________ is hereby authorised to submit the Bid documents, in sealed format to participate in tender and to sign the contract on behalf of our organisation for all the services / systems/ goods required by the bank as called for vide the bank's request for proposal vide RFP ____________ dated ___________ on behalf of our organization.

We confirm that all the prices quoted in tender by him shall be binding on us. He/ She is also authorised to take decisions on behalf of the company till RFP process is completed. Certified Xerox copy of Power of Attorney (P/A) of the person authorising such person is duly submitted.
We hereby extend our full guarantee and warranty as per Clauses of Contract for the goods and services offered against this RFP.

The specimen signature is attested below:

____
Specimen Signature of Representative

____

Signature of Authorizing Authority

Name of Authorizing Authority (Certified Xerox copy of P/A of authorised Signatory/authority is to be submitted)

Note: 1. This letter of authority should be on the letterhead of the Bidder on whose behalf the proposal is submitted and should be signed by a person competent and having the power of attorney to bind the principal. It should be included by the Bidder in their Bid.

7. ANNEXURE VII – Non-Blacklisting

(on Organisation's letterhead)

To the best of our knowledge and as per records available with the Company, we hereby declare that we have not been placed on any black list, declared by any Bank, Financial Institution, Govt's Bidder Black List, except as indicated below:

(Here give particulars of black listing and in the absence thereof state "NIL")

It is also understood that if this declaration is found to be false in any particular, NABARD shall have the right to reject my/our Bid, and if the Bid has resulted in a contract, the contract is liable to be terminated.

Signature of Bidder:__________________________

Place:

Date:

Name of Signatory: __________________________

8. ANNEXURE VIII – Earnest Money Deposit/Bid Security Form

Ref No............ Dated: --/--/2022

The Chief General Manager
Department of Information Technology,
National Bank for Agriculture and Rural Development
5th Floor, C Wing, C-24, 'G' Block, Bandra-
Kurla Complex, P.B. No. 8121, Bandra (East),
Mumbai – 400 051
Maharashtra

Dear Sir

WHEREAS the National Bank for Agriculture and Rural Development, a body corporate established under the NABARD Act, 1981 (hereinafter referred to as NABARD, which expression shall, include its successors and assigns) has invited tenders for Comprehensive IT Services mangement for NABARD.

(2) WHEREAS M/s_____________________________________ who are our constituents (hereinafter referred to as "the Tenderers", which expression shall include the successors and assigns) have taken the tender for the said work.

(3) AND WHEREAS it is one of the condition of the said tender that the Tenderer shall deposit with the NABARD at the time of submitting the tender a sum of `-------- /- (Rupees --- only) as and by way of Bid Security (BS), which BS shall not bear any interest and which shall be liable for forfeiture in the event of the Tenderer, after acceptance of his tender by NABARD, failing to observe any of the terms and conditions of the tender or the Tenderer not supplying the said software to the satisfaction of NABARD and / or its Consultants.

(4) AND WHEREAS at the request of the Tenderer, NABARD has agreed not to insist for payment of the said BS in cash and accept the guarantee from a Scheduled Commercial Bank in lieu thereof and have agreed to accept the same from us, the Bank i.e. __________________ (Name of the bank) on behalf of the tenderer, as hereinafter contained.

In the premises aforesaid and in consideration of NABARD having agreed at our request to exempt the tenderer from depositing the said BS in cash. We,___________________________Bank having our Head Office at ____________________and one of our Branches at ____________________do hereby unconditionally and irrevocably guarantee unto the NABARD that the Tenderer will execute the Agreement soon upon acceptance of the tender by NABARD and will diligently, efficiently and satisfactorily perform all their obligations under the various terms and conditions of the said tender (read with any amendments made thereto by mutual consent of NABARD and the Tenderer) and supply the said software in the satisfaction of the NABARD / its Consultants within the time stipulated therein, failing which WE the____________________________Bank shall, on demand and without demur, pay unto the NABARD the sum of ` --------------/- (Rupees-- only) at its office at Mumbai.

We ____Bank further covenant that:

(a) We shall pay the aforesaid sum on demand made in writing by NABARD without reference to the Tenderers and notwithstanding any dispute or difference that may exist or arise between the NABARD and the Tenderers;

(b) that this guarantee shall be a continuing guarantee and shall not be revoked by us without prior consent in writing of NABARD.

(c) that the decision of NABARD on the breach of any of the terms and conditions of the said contract / tender by the Tenderers or their failure to perform their obligations or discharge their duties under the said tender / contract shall be final and binding on us and shall not be disputed by us inside or outside the court, tribunal, arbitration or other authority;

(d) that the notice of demand in writing issued by NABARD shall be conclusive proof as regards the amount due and payable to NABARD under this guarantee and it shall not be disputed by us either inside or outside the court, tribunal or arbitration or other authority;

(e) that any neglect or forbearance on the part of NABARD in enforcing any of the terms and conditions of the said tender / contract or any indulgence shown by NABARD to the Tenderer or any variation in the said tender / contract terms made by mutual agreement between NABARD and the Tenderer or any other act or deed on the part of NABARD which but for this clause may have the effect of discharging us under the law relating to guarantee / sureties shall not discharge us from our obligations herein and we shall be discharged only by compliance by the Tenderers with all their obligations / duties under the said tender / contract or by payment of the sum.

(f) that this guarantee shall not be affected by any infirmity or absence or irregularity in the exercise of the powers by or on behalf of the tenderers to submit the said tender and enter into the said contract or any change in the constitution or dissolution of the Tenderers or change in its name;

(g) that it shall not be necessary for NABARD to exhaust its remedies against the Tenderers before invoking this guarantee and the guarantee therein contained shall be enforceable against us notwithstanding any other security which the NABARD may have obtained or may hereafter be obtained from the Tenderers at the time when this guarantee is invoked is outstanding and unrealized;

(h) that we hereby agree that this guarantee shall be valid and be in force for a period of 180 days, i.e. up to ___________ and we hereby agree to renew this guarantee for such further period or periods at the request of NABARD in the event of the works specified in the Tender are finally awarded to the Tenderers and / or the works awarded are not completed within the stipulated period and such renewal shall be entirely at the cost and expense of the Tenderer.

(i) Any claim arising under this guarantee shall be preferred by NABARD within a period of six months from the aforesaid date of expiry i.e.____________ or, in the event of any renewal, within a period of six months from the date of expiry of such renewed period extended by such renewal, and unless the claim is so preferred against us, we shall stand discharged of all our liabilities hereunder.

Yours faithfully

For and on behalf of

____________________ **Bank**

(Authorized Official)

All Confidential Information shared pursuant to the NDA is required to maintained as confidential in perpetuity unless such information falls within the exceptions set out therein.

9. ANNEXURE IX – Pre-Contract Integrity Pact

(To be executed on Non-Judicial Stamp Paper of `100/-)

Between

National Bank for Agriculture and Rural Development (NABARD)
hereinafter referred to as **"The Buyer"**
And

.... hereinafter referred to as **"The Bidder"**

Preamble

The Buyer intends to award, under laid down organizational procedures, contract/s for .... The Buyer values full compliance with all relevant laws of the land, rules, regulation, and economic use of resources and of fairness /transparency in its relations with its Bidder(s) and/or Contractor(s).

In order to achieve these goals, the Buyer will appoint Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Buyer

(1) The Buyer commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a. No employee of the Buyer, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Buyer will, during the tender process treat all Bidder(s) with equity and reason.
The Buyer will, in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Buyer will exclude from the process all known prejudiced persons.

(2) If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Buyer will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/Contractor(s)

(1) The Bidder(s) / Contractor(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s) / Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution:

a. The Bidder(s) / Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of Bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act or any other applicable anti-corruption laws; further the Bidder(s) / Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign Buyers, if any.

e. The Bidder(s) /Contractor(s) will, when presenting their Bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f. Bidder(s) /Contractor(s) who have signed the Pre- Contract Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s) /Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 – Disqualification from tender process and exclusion from future contracts

If the Bidder(s) /Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form which put their reliability or credibility in question, the Buyer is entitled to disqualify the Bidder(s) /Contractor(s) from the tender process.

Section 4 – Compensation for Damages

(1) If the Buyer has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Buyer is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

(2) If the Buyer has terminated the contract according to Section 3, or if the Buyer is entitled to terminate the contract according to Section 3, the Buyer shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption/ Transparency International (TI) approach or with any Public Sector Enterprise in India/ Undertaking in India or any Government Department in India.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process and/or an action for his exclusion may taken and/or he shall be liable for compensation of such damages that are incidental to such transgression mentioned herein.

Section 6 – Equal treatment of all Bidders / Contractors/ Subcontractors

(1) In case of sub-contracting, the Contractor shall take the responsibility of the adoption of Pre- Contract Integrity Pact by the sub-contractor and shall submit the same to the Buyer before contract signing.

(2) The Buyer will enter into agreements with identical conditions as this one with all Bidders and Contractors

(3) The Buyer will disqualify from the tender process all Bidders who do not sign the Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s)/ Subcontractor(s)

If the Buyer obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor

(1) The Buyer appoints competent and credible Independent External Monitor (“**Monitor**”) for this Pre- Contract Integrity Pact after approval by the Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

The Independent External Monitor appointed for NABARD is:

Shri Pramod Kumar Sangewar, IRSS (Retd)
H No. 12-5-65/1, Flat No 109,
Shri Harsha Sethuram Unique,
Vijaypuri Colony, South Lalaguda,
Secunderabad,
Telangana - 500 017

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor

would have the right to access all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidders /Contractors as confidential. He / she reports to the Chairman, NABARD.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Buyer including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s) /Contractor(s) / Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on 'Non-disclosure of Confidential Information and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform Chairman, NABARD and recuse himself/herself from that case.

(5) The Buyer will provide to the Monitor sufficient information about all meetings among the parties related to the Project, provided such meetings could have an impact on the contractual relations between the Buyer and the Bidder/Contractor/Sub-Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Buyer and request the Management to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the Chairman, NABARD within 8 to 10 weeks from the date of reference or intimation to him by the Buyer and, should the occasion arise, submit proposal for correcting problematic situations.

(8) If the Monitor has reported to the Chairman, NABARD, a substantiated suspicion of an offence under the relevant IPC/PC Act or any other statutes/laws, and the Chairman NABARD has not, within reasonable time, taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word **'Monitor'** would include both singular and plural.

Section 9 – Pact Duration

This Pre- Contract Integrity Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract and for all other third party/OEM Bidders after 6 months. Any violation of the same would entail disqualification of the Bidders and exclusion from future business dealings.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharge/determined by the Chairman of NABARD.

Section 10 – Other provisions

(1) This agreement is subject of Indian Laws, place of performance and jurisdiction is the Head Office of the Buyer, i.e. Mumbai.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a consortium, this agreement should be signed by all consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) Issues like Warranty/Guarantee etc. shall be outside the purview of IEMs.

(6) In the event of any contradiction between the Integrity Pact and its Annexure, if any, the Clause in the Integrity Pact will prevail.

BUYER	Bidder
Name of the Officer	Chief Executive Officer
Designation	Organisation
NABARD	
Witness	Witness
1.________________________	1. ________________________
2.________________________	2.________________________

10. ANNEXURE X – Statement of Deviations

The Statement of Deviation allows a Bidder to request for deviations in their scope of work. The specific clause referred to in Annexure I is a representation that the Bidder will abide by all terms of the RFP.

Bidder is required to provide details of all deviations, comments and observations or suggestions in the following format with seal and signature. It also needs to provide a reference of the page number, state the clarification point as stated in tender document and the comment/ suggestion/ deviation that you propose as shown below.

NABARD may at its sole discretion accept or reject all or any of the deviations, however it may be noted that the acceptance or rejection of any deviation by NABARD will not entitle the Bidder to submit a revised Technical or Commercial Bid.

Tender No: No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022

Sr. NO.	Page Number	Section Number	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation
1.				
2.				
3.				
4				
5				
6				

Authorized Signatories

Name: ___________________________________

Designation: _____________________________

Company Seal:

11. ANNEXURE XI – Bank Mandate Form

(To be submitted in Duplicate)

1.	Name of Bidder/Organisation			
2	Address of the Bidder/Organisation			
	City		E-mail id	
	Pin Code		Mobile: No.	
	Phone No. with STD code			
3	Permanent Account Number			
4	GST Number			
5	MSE Registration / CA Certificate 3 (if applicable)			

6. **Particulars of Bank account:**

Beneficiary Name				
Bank Name		Branch Name		
Branch Place		Branch City		
PIN Code		Branch Code		
MICR No.				
Account type	Saving	Current	Cash Credit	
Account No. ***(as appearing in the Cheque book)***				
Please attach a cancelled cheque of your bank for ensuring accuracy of the bank name, branch name & code and Account Number				
IFSC CODE	For transfer RTGS		For transfer NEFT	

7. I hereby declare that the particulars given above are correct and complete. If any transaction is delayed or not effected for reasons of incomplete or incorrect information, I shall not hold NABARD responsible. I also undertake to advise any change in the particulars of my account to facilitate updation of records for purpose of credit of amount through RBI RTGS/NEFT.

Place : _______________

Date : _______________

Signature of the party / Authorized Signatory

Certified that particulars furnished above are correct as per our records.

Bank's stamp

(Signature of the Authorized Official from the Bank's)
Date :

12.ANNEXURE XII – Compliance Statement

(To be submitted on Bidder's letter head)

Declaration

Tender No. No.NB.HO.DIT/25 /DIT-19-01/2022-23 dated 12 May 2022

Compliance	**Description**	**Bidder Response (Yes/ No)**
Special Terms & Conditions, General Terms & Conditions	We hereby undertake and agree to abide by all the terms and conditions including annexures, corrigendum(s) etc. stipulated by the Bank in this RFP. (Any deviation may result in disqualification of Bids)	
Scope of Work	We certify that the proposal submitted by us is as per the scope of work stipulated in the RFP. (Any deviation may result in disqualification of Bids)	

Bank reserves the right to reject the Bid, if the Bid is not submitted in proper format as per RFP.

Authorized Signatories

Name: ___________________________________

Designation: _____________________________

Company Seal:

Date:

13. ANNEXURE XIII – Non Disclosure Agreement

(To be executed on a non-judicial stamped paper of requisite value based on place of execution)

This Non-Disclosure Agreement made and entered into at ………………… this……. day of ……………….. 2022 BY AND BETWEEN ………………………………. Company Limited, a company incorporated under the Companies Act, 1956 / 2013 having its registered office at …………. (hereinafter referred to as the **"Bidder"**, which expression unless repugnant to the context or meaning thereof be deemed to include its permitted successors) of the ONE PART;

AND

National Bank for Agriculture and Rural Development, a body corporate established under an act of Parliament, viz., National Bank for Agriculture and Rural Development Act, 1981 having its registered office at NABARD Head Office, C-24, "G" Block, Bandra Kurla Complex, Bandra (East), Mumbai- 400051 (hereinafter referred to as "NABARD" which expression shall unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the OTHER PART.

The Bidder and NABARD are hereinafter collectively referred to as "Parties" and individually as "Party".

WHEREAS:

1. NABARD is engaged in Banking business and floated a Request for Proposal to appoint a Bidder for Comprehensive IT Services Management, the scope of which is specified in RFP Ref No. NB.HO……………… 2022 and whereas

2. The Bidder proposes to Bid for the work through an RFP process. In the course of such assignment, it is anticipated that NABARD or any of its officers, employees, officials, representatives or agents may disclose, or deliver, to the Bidder some Confidential Information (as hereinafter defined), to enable the Bidder to carry out the aforesaid exercise (hereinafter referred to as " the Purpose").

NOW, THEREFORE THIS AGREEMENT WITNESSETH THAT in consideration of the above premises and NABARD granting the Bidder and or his agents, representatives to have specific access to NABARD property / information and other data it is hereby agreed by and between the Parties hereto as follows:

1. Definitions

(i) "Confidential Information" means all information that NABARD designates as being confidential or which the circumstances surrounding the disclosure ought to be treated as confidential. It includes all information disclosed/furnished by NABARD or any such information which comes into the knowledge of the Bidder during the course of engagement, whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the Bidder to carry out the assignment, and shall mean and include, without limitation (1) data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; (2)information relating to installed or purchased Disclosing Party material or hardware products, the information relating to general architecture of Disclosing Party's Comprehensive IT Services mangement, information relating to nature and content of data stored within Comprehensive IT Services mangement or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement; (3)Information such as any trade secrets, discoveries, ideas, concepts, techniques, materials, formulae, compositions, information, data, results, plans, surveys and/or reports of a technical nature or concerning research and development and/or engineering activity, commercial, financial, scientific or technical information, patent and trademark applications, process designs, process models, drawings, plans, designs, data, databases and extracts there from, formulae, methods, know-how and other intellectual property, marketing and pricing information, and other strategies, concepts, ideas; (4) technical or business information or material not covered in (i); (5) proprietary or internal information relating to the current, future and proposed products or services of NABARD including, financial information, process/flow charts, business models, financial reports, business plans, customer lists, products or production processes, designs, drawings, data information related to products and services, procurement requirements, purchasing, customers, investors, employees, business and contractual relationships, business forecasts, business plans and strategies, information the Parties provide regarding third parties; (6) information disclosed pursuant to this agreement including but not limited to Information Security policy and procedures, internal policies and plans and Organization charts etc.; and (7) all such other information which by its nature or the circumstances of its disclosure is confidential Confidential Information in oral form should be identified as confidential at the time of disclosure and confirmed as such in writing within fifteen days of such disclosure

(ii) “Intellectual Property Rights” means any patent, copyright, trademark, trade name, design, trade secret, permit, service marks, brands, propriety information, knowledge, technology, licenses, databases, computer programs, software, know-how or other form of intellectual property right, title, benefits or interest whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.

2. Confidentiality

i) The Bidder may use the Confidential Information solely for and in connection with the Purpose and shall not use the Confidential Information or any part thereof for any reason other than the Purpose stated above. Bidder shall not, without prior written permission of NABARD, use or disclose for its own or any third party’s benefit any Confidential Information received hereunder for purposes other than the Purpose.

ii) Confidential Information shall at all times remain the sole and exclusive property of NABARD. Upon termination of this Agreement, Confidential information shall be returned to NABARD or destroyed at its directions. The destruction of information if any, shall be witnessed and so recorded, in writing, by an authorised representative of each of the Parties. Nothing contained herein shall in any manner impair or affect rights of NABARD in respect of the Confidential Information.

iii) All Confidential Information of NABARD remains the exclusive property of NABARD and Bidder acknowledges and agrees that nothing contained in this Agreement will be construed as granting any rights, by license or otherwise, to any Confidential Information, except as expressly specified in this Agreement with respect to the Purpose. Bidder nor any of its employees or agents shall attempt to acquire or appropriate any right or title in or to the Confidential Information whether by means of patent application or otherwise.

iv) In the event Bidder is legally compelled to disclose any Confidential Information in a judicial, administrative or governmental proceeding, Biddder shall give sufficient notice of 45 days to NABARD to prevent or minimize to the extent possible, such disclosure. Bidder shall disclose to third party i.e. any Confidential

Information or the contents of this Agreement without the prior written consent of NABARD. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Bidder will apply to its own similar confidential information but in no event less than reasonable care. The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement.

v) Further disclosure of Confidential Information received hereunder shall be limited to Bidder's employees who need access to the Confidential Information for the performance of activities related to this Agreement and the RFP and prior to the disclosure of any Confidential Information, Bidder shall inform each employee of the confidential nature of the Confidential Information and shall expressly require that the employee agrees to handle the Confidential Information in accordance with this Agreement. Each Party shall be fully responsible for any breach of any obligation of secrecy or limited use by its employees.

vi) Bidder may disclose Confidential Information to its Affiliates if and to the extent this is required to achieve the Purpose provided that such Affiliates are bound by obligations of confidentiality and limited use at least as restrictive as those set forth herein, and further provided that any breach thereof by such Affiliates shall be deemed a breach by Bidder hereunder.

vii) The Bidder agrees to notify NABARD immediately if it learns of any use or disclosure of the Confidential Information in violation of terms of this Agreement.

viii) Confidential Information does not include information which as is shown by competent written evidence:

(a) Is or subsequently becomes legally and publicly available without breach of this Agreement or the RFP, at the time of disclosure.

(b) After disclosure, becomes part of the public domain by publication or otherwise through no fault or breach by the Bidder.

(c) was rightfully in the possession of the Bidder without any obligation of confidentiality prior to receiving it from NABARD, or prior to entering into this RFP. The recipient shall have the burden of proving the source of information herein above mentioned.

(d) was rightfully obtained by the Bidder from a source other than NABARD without any obligation of confidentiality,

(e) was developed by for the Bidder independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

(f) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.

(g) is released from confidentiality with the prior written consent of the other Party.

The Receiving Party shall have the burden of proving hereinabove are applicable to the information in the possession of the recipient.

3. Publications

The Bidder shall not make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this RFP, the contents / provisions thereof, other information relating to this Agreement, including references whether through media, social network or otherwise, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of NABARD.

4. Term

This Agreement shall be effective from the date of execution hereof and shall continue till expiration of the Purpose or termination of this Agreement by NABARD, whichever is earlier. The Biddder hereby agrees and undertakes to NABARD that immediately on termination of this Agreement it would forthwith cease using the Confidential Information and further as directed NABARD promptly return or destroy, under information to NABARD, all information received by it from NABARD for the Purpose, whether marked Confidential or otherwise, and whether in written, graphic or other tangible form and all copies, abstracts, extracts, samples, notes or modules thereof. The Bidder further agrees and undertake to NABARD to certify in writing to NABARD that the obligations set forth in this Agreement have been fully complied with.

Obligation of confidentiality contemplated under this Agreement shall continue to be binding and applicable for a period of five year years after the expiry or termination of the agreement, whichever is earlier.

5. Title and Proprietary Rights

Notwithstanding the disclosure of any Confidential Information by NABARD to the Bidder, the title and all intellectual property and proprietary rights in the Confidential Information shall remain with NABARD. Inventions, improvements or discoveries made by Bidder using any Confidential Information hereunder as well as all intellectual property rights arising in this connection shall be the sole and absolute property of NABARD. Bidder shall promptly notify NABARD in writing of any such invention, improvement or discovery and assign and transfer to NABARD promptly and all right and title in such invention, improvement or discovery. Bidder shall be compensated for the invention, improvement or discovery in case such is being used by NABARD for commercial usage.

6. Return of Confidential Information

Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all the copies, materials, abstracts, extracts, samples, notes, modules thereof, all analyses, summaries, memoranda or other notes made by the Bidder, and all other physical or electronic media containing Confidential Information, except for one copy which may be retained by an authorized legal representative of the Bidder solely for purposes of assuring compliance hereunder and except that electronic data comprised of Confidential Information of NABARD, as stored on Bidder's electronic data systems to the Disclosing Party within seven (07) days after receipt of notice, and (iii) upon request of Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.

7. Remedies

7.1 The Bidder acknowledges the confidential nature of Confidential Information and breach of any provision of this Agreement by the Bidder will result in irreparable damage to NABARD for which monetary compensation may not be adequate and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof. NABARD shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the Bidder, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement. Any claim for relief to NABARD shall include NABARD's costs and expenses of enforcement (including the attorney's fees).

7.2 The Bidder shall notify NABARD immediately upon discovery of any unauthorized used or disclosure of Confidential Information, and will cooperate with NABARD in every reasonable way to help NABARD regain possession of the Confidential Information and prevent further unauthorized use thereof.

7.3 The Bidder acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that NABARD shall be entitled, without waiving any of its rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction, NABARD shall also have the right to impose the following consequences on the Bidder.

a. Suspension of access privileges for Bidder
b. Requiring the Bidder to change personnel assigned to the relevant job in relation to which breach has occurred;
c. Financial liability for all direct damages which NABARD has incurred as a result of breach of the terms of this Agreement by the Bidder or its employees or advisors or representatives.

NABARD may visit the Bidder's premises, with reasonable prior notice and during normal business hours, to review the Bidder's compliance with the term of this Agreement. The particulars of visit and verification of the relevant documents shall be decided by NABARD and communicated to the Bidder with prior intimation.

8. Entire Agreement, Amendment, Assignment

This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements relating to non-disclosure between the parties. The Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

Neither Party shall be obligated to the other hereunder to enter into any further contractual arrangements. Disclosure of Confidential Information hereunder shall be limited to the Purpose; and further agreements, if any, shall be subject to terms and conditions to be mutually agreed by both Parties.

9. Miscellaneous

9.1 Any software, material and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

9.2 Neither Party grants to the other Party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the Parties, or any license rights whatsoever in any patent, copyright or other Intellectual Property rights pertaining to the Confidential Information.

9.3 For the purpose of avoiding any ambiguity it is clarified that the services / solution or other deliverables provided or to be provided by the Bidder to Bank shall be the property of the Bank and shall be considered as confidential information of the Bank. The Bidder shall not be disclosing such details to any third parties without having the express written permission of the Bank.

9.4 This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of a Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

9.5 NABARD makes no representation or warranty whether express or implied, with respect to the accuracy, truthfulness, completeness lawfulness, and merchantability, fitness for a particular purpose, title, non-infringement, or anything else of any Confidential Information provided to Bidder hereunder and Bidder agrees that NABARD and its Affiliates shall not incur any liability to Bidder as a result of Bidder's use of or reliance on the Confidential Information hereunder.

9.6 In witness whereof, the Parties hereto have executed these presents the day, month and year first herein above written

9.7 Nothing contained herein shall be deemed to be an obligation on NABARD to disclose any Confidential Information.

9.8 Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns.

9.9 If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect. All obligations created by this Agreement shall survive change or termination of the Parties' business relationship.

10. Suggestions and Feedback

Either Party from time to time may provide suggestions, comments or other feedback to the other Party with respect to Confidential Information provided originally by the other Party (hereinafter "**Feedback**"). Both Parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the Receiving Party. However, the Receiving Party shall not disclose the source of any Feedback without the providing Party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each Party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other Party. The foregoing shall not, however, affect either Party's obligations hereunder with respect to Confidential Information of other Party.

11. Governing Law

The provisions of this Agreement shall be governed by the laws of India and the competent court at Mumbai shall have exclusive jurisdiction in relation thereto even though other Courts in India may also have similar jurisdictions.

BUYER	Bidder
Name of the Officer	Chief Executive Officer
Designation	Organisation
NABARD	

Witness

1.________________________	1.________________________
2.________________________	2.________________________

14.ANNEXURE XIV –Performance Bank Guarantee Format

(to be executed on a non-judicial stamped paper of appropriate value)

In consideration of National Bank for Agriculture and Rural Development (NABARD) having Head Office at C-24, G-Block, Bandra-Kurla Complex, P.O. Box No.8121, Bandra (E), Mumbai – 400 051 (hereinafter referred to as "Purchaser") having agreed to undertake Comprehensive IT Services mangement for NABARD (hereinafter referred to as "Services") from ________________________ (hereinafter referred to as "Contractor") on the terms and conditions contained in the RFQ (Ref. No.______ Dated_________) and their agreement (hereinafter referred to as the "Contract") and subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the Comprehensive IT Services mangement (hereinafter referred to as "Proposed Services") as per the terms and conditions as set forth in the said Contract and also guaranteeing the Proposed Services as per the terms and conditions of the said Contract;

1) We, --------------------------- (Bank) (hereinafter called "the Bank"), in consideration of the premises and at the request of the Contractor, do hereby guarantee and undertake to pay to the Purchaser, forthwith on mere demand and without any demur, at any time up to ____________ 2022 (validity date of BG) money or monies not exceeding a total sum of Rs _______/- (Rupees ____________only) as may be claimed by the Purchaser to be due from the Contractor by way of loss or damage caused to or would be caused to or suffered by the Purchaser on failure of the Contractor to provide Proposed Services as per the terms and conditions of the said Contract ("**Guarantee**").

2) Notwithstanding anything to the contrary, the decision of the Purchaser as to whether the Contractor has failed to provide Proposed Services as per the terms and conditions of the said Contract will be final and binding on the Bank and the Bank shall not be entitled to ask the Purchaser to establish its claim or claims under this Guarantee but shall pay the same to the Purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/ or without any reference to the Contractor. Any such demand made by the Purchaser on the Bank shall be conclusive and binding notwithstanding any difference between the Purchaser and the Contractor or any dispute pending before any Court, Tribunal, arbitrator, or any other authority.

3) This Guarantee shall expire on ___________2027 (validity date) without prejudice to the Purchaser's claim or claims demanded from or otherwise notified to the Bank in writing on or before the said date i.e. ____________ 2027.

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the Purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the Purchaser under or by virtue of the said Contract have been duly paid and its claims satisfied or discharged or the Purchaser certifies that the terms and conditions of the said Contract have been fully carried out by the Contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, the Purchaser shall be entitled to act as if we are Purchaser's principal debtors in respect of all the claims of the Purchaser against the Contractor hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety-ship and other rights, if any, which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the Purchaser that the Purchaser shall have the fullest liberty without affecting, in any manner, the Bank's obligations under this Guarantee to extend the time of performance by the Contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the Purchaser against the Contractor and either to enforce or forbear to enforce any of the terms and conditions of the said Contract, and the Bank shall not be released from its liability for the reasons of any such extensions being granted to the Contractor for any forbearance, act or omission on the part of the Purchaser or any other indulgence shown by the Purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision, have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the Contractor or the Bank nor shall it be affected by any change in the constitution of the Purchaser by any amalgamation or absorption or with the Contractor, Bank or the Purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by the Bank (whether singly or jointly with other banks) on behalf of the Contractor heretofore mentioned for the same Contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing uncancelled and the Bank further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by the Bank on behalf of the Contractor heretofore mentioned for the same Contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax, e-mail or registered post to the local address of the Bank as mentioned in this guarantee.

10) Notwithstanding anything contained herein:-

i. Our liability under this Guarantee shall not exceed ₹. _____/- (Rupees ___________only) ;

ii. This Guarantee shall be valid up to ___________(validity date) ;

iii. Unless actions to enforce the claims is filed on or before ______ ______ (validity date) all rights under the said Guarantee shall be forfeited and Bank shall be relieved and discharged from all liabilities thereunder.

iv. The Bank is liable to pay the guaranteed amount or any part thereof under this Guarantee only and only if the Purchaser serves upon the Bank a written claim or demand on or before _________ (validity date)

11) The Bank has power to issue this Guarantee under the statute/ constitution and the undersigned has full power to sign this Guarantee on behalf of the Bank. Date this ------------------- day of ----------------- 2022 at ----------

For and on behalf of ------------------------- Bank.

sd/- --------------------------------

Dated this ------- ----- day of --------------- 2022 at

For and on behalf of ------------------- —-— Bank.

Sd/______

15. ANNEXURE XV – Contract Form

(to be executed on Non-judicial stamp paper of appropriate value)

National Bank for Agriculture and Rural Development (NABARD), a Body Corporate established under the National Bank for Agriculture and Rural Development Act, 1981, and having its Head Office at C-24, G Block, Bandra Kurla Complex (BKC), Bandra (E), Mumbai - 400 051 (hereinafter called the Bank / Purchaser, which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successor and assignee) of one part; and

M/s ______________________ (Name of the Bidder/Service Provider), a Company/a Firm/ duly registered/incorporated ________________________ Act, having its Registered Office/ Head Office/ Corporate Office at ______________________________ (City & Country of Bidder/Supplier) (hereinafter referred to as the "the Supplier" / "Bidder", which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assignee) of Other Part.

WHEREAS the Purchaser is desirous that services related to Comprehensive IT Services mangement for the Bank should be provided by the Supplier viz., _________________ _________________ (Brief Description of Goods, Services and Consultancy) and has accepted a Bid by the Supplier for Comprehensive IT Services mangement for the Bank in the sum of ₹________________________________ (Contract Price in Words and Figures) (hereinafter "the Contract Price").

NOW THEREFORE, in consideration of the mutual agreements, covenants, representations and warranties set forth in the Agreement, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, the Parties hereby agree as follows:

1. In this Contract words and expressions shall have the same meanings as are respectively assigned to them in RFP.
2. The following documents shall be deemed to form and be read and construed as part of this Contract along-with RFP, viz.:

   a) The Bid form, price schedule and all other documents submitted by the Bidder in response to the RFP;

   b) The Scope of Work;

   c) The special terms and conditions provided under the RFP;

   d) The Service Level Agreement;

   e) The general terms and conditions provided under the RFP;

   f) The Purchaser's Notification of Award

   However, in case of any conflict clauses between this Contract and the RFP or its enclosures, the provisions of RFP shall prevail.
3. In consideration of the Contract Price, the Supplier hereby covenants with the Purchaser to provide the Services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the Services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

5. Brief particulars of the Sservices which shall be supplied/provided by the Supplier are as set out in Exhibit I, attached hereto.

6. Independent Contractor

This Contract does not set up or create an employer/employee relationship, partnership of any kind, an association or trust between the Parties, each Party being individually responsible only for its obligations as set out in this Agreement. Parties agree that their relationship is one of independent contractors. Neither Party is authorised or empowered to act as agent for the other for any purpose and neither Party shall on behalf of the other enter into any contract, warranty or representation as to any matter. Neither Party shall be bound by the acts or conduct of the other. Employees/workmen of neither Party shall be construed or treated as the workmen/employees of the other Party or place any obligation or liability in respect of any such workmen/employee upon the other Party, including without limitation, worker's compensation, disability insurance, leave or sick pay.

7. Dispute Resolution, Governing Law and Jurisdiction

7.1 This Agreement shall be governed by the laws of India.

7.2 All disputes and differences of any kind whatsoever, arising out of or in connection with this Agreement or in the discharge of any obligation arising under this Agreement (Whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Agreement) shall be resolved amicably by Parties. Each Party shall select / appoint 1 (one) senior representative. Such discussions towards amicable settlement of the dispute shall be undertaken for a period of 30 days from the date of appointment of both the respective senior representatives ("**Settlement Period**").

7.3 In case of failure to resolve the disputes and differences amicably as per the mechanism set out in Clause 7.2 prior to expiry of the Settlement Period, such unsettled dispute or difference shall be referred to and finally resolved by arbitration administered by the Mumbai Centre for International Arbitration in accordance with the Arbitration Rules of the Mumbai Centre for International Arbitration ("MCIA Rules") for the time being in force, which rules are deemed to be incorporated by reference in this Clause 20 (Dispute Resolution, Governing Law and Jurisdiction). In the event of such arbitration:

7.3.1 the venue and seat of the arbitration shall be Mumbai;

7.3.2 the tribunal shall consist of 3 (three) arbitrators; 1 (one) to be appointed by the Bank, 1 (one) to be appointed by the Supplier, and the third to be appointed by the 2 (two) arbitrators. If either the Bank or the Supplier fails to appoint an arbitrator as set out in this Clause 7 (Dispute Resolution, Governing Law and Jurisdiction), the arbitrator of such party shall be appointed in accordance with the MCIA Rules;

7.3.3 the language of the arbitration shall be English;

7.3.4 the arbitration awards shall be reasoned and shall be final and binding on the disputing Parties and may be specifically enforced by any court of competent jurisdiction;

7.3.5 the tribunal shall be entitled to decide on and apportion the costs and reasonable expenses (including reasonable fees of counsel retained by the Parties) incurred in the arbitration;

7.3.6 the existence and content of any arbitration proceeding, and any award thereof shall be confidential among the Parties, and subject to the terms of Clause 10 (Confidentiality) of the RFP; and

7.3.7 the existence or subsistence of a dispute between the Parties, or the commencement or continuation of arbitration proceedings, shall not, in any manner, prevent or postpone the performance of those obligations of Parties under the Agreement which are not in dispute, and the arbitrators shall give due consideration to such performance, if any, in making a final award.

7.4 Notwithstanding anything in the contrary set forth in this Agreement, each Party shall be entitled to seek urgent interim relief in any court of competent jurisdiction, including pre-arbitral attachments, temporary restraining orders, or temporary injunctions, as may be necessary to preserve the rights of such Party. The application by either Party to a judicial authority for such measures shall not be deemed to be an infringement or a waiver of the covenant of the Parties to submit disputes to arbitration under this Agreement and shall not affect the relevant powers reserved to the arbitrator pursuant to this Clause 20 (Dispute Resolution, Governing Law and Jurisdiction).

7.5 All disputes arising out of or in any way connected with this Agreement shall be deemed to have arisen at Mumbai only and subject to the arbitration provisions above, courts in Mumbai only shall have jurisdiction to determine the same.

8. SEVERABILITY

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be separable from the remainder of the provisions hereof which will continue in full force and effect as if this Agreement had been executed with the invalid provisions eliminated.

9. WAIVER

The failure of either Party to insist upon strict performance of any provision of this Agreement, or the failure of either Party to exercise any right or remedy to which it is entitled hereunder or thereunder, will not constitute a waiver thereof and will not cause a diminution of the obligations established by this Agreement. A waiver of any default will not constitute a waiver of any subsequent default. No waiver of any of the provisions of this Agreement will be effective unless it is expressly stated to be a waiver and communicated to the other Party in writing.

10. COUNTERPARTS

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument and any Party may execute this Agreement by signing any one or more of such originals or counterparts. The delivery of signed counterparts by facsimile transmission or electronic mail in “portable document format” (“.pdf”) shall be as effective as signing and delivering the counterpart in person.

11. ENTIRE AGREEMENTAND AMENDMENTS

11.1 This Agreement shall be deemed to be incorporated as part of the Principal Agreement by reference. This Agreement along with the Principal Agreement shall contain the entire understanding of the Parties and shall supersede all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter hereof.

11.2 No supplement, amendment or modification to this Agreement shall be valid, enforceable or binding upon the Parties unless made in accordance with the provisions of this Agreement.

12. FURTHER ASSURANCE

The Parties shall do or procure to be done all such further acts and things and execute or procure the execution of all such other documents as reasonably required to give effect to the provisions of this Agreement.

13. NOTICES

13.1 Any notice or other communication to be given by one Party to any other Party under, or in connection with, this Agreement shall be made in writing and signed by, or on behalf of, the Party giving it.

13.2 Service of a notice shall be effected by one of the following methods:

13.2.1 by hand to the relevant address set out in Clause 13.4 (Address for Service) and shall be deemed served upon delivery if delivered during a Business Day, or at the start of the next Business Day if delivered at any other time; or

13.2.2 by prepaid first-class post to the relevant address set out in Clause 13.4 (Address for Service) and shall be deemed served at the start of the second Business Day after the date of posting; or

13.2.3 by prepaid international airmail to the relevant address set out in Clause 13.4 (Address for Service) and shall be deemed served at the start of the fourth Business Day after the date of posting; or

13.2.4 by email, to the relevant email address set out in Clause 13.4 (Address for Service) and shall be deemed served on the day when the sending of the email is recorded on the sender's computer, unless the sender receives a message from its internet service provider or the recipient's mail server indicating unsuccessful transmission. Any such email should be followed by service of the notice through one of the methods in 13.2.1 through 13.2.3, within 3 (three) Business Days of such email being deemed as served pursuant to this sub-13.2.4.

13.3 In Clause 13.2 (Method of Service), "during a Business Day" means any time between 9.30 am and 5.30 pm on a Business Day based on the local time where the recipient of the notice is located. References to "the start of a Business Day" and "the end of a Business Day" shall be construed accordingly.

13.4 Notices shall be addressed as follows:

In case of notice to the Bank

Name: [Insert]

Address : [Insert]

Email address : [Insert]

To the attention of : [Insert]

In case of notice to Supplier

Name: [Insert]

Address : [Insert]

Email address : [Insert]

To the attention of : [Insert]

13.5 Either Party may, from time to time, change its address or representative for receipt of notices provided for in this Agreement by giving to the other Party not less than 7 (Seven) Business Days' prior written notice. Until the end of such notice period, service on either address shall remain effective.

14. SPECIFIC PERFORMACE

The Parties agree that each Party shall be entitled to an injunction, restraining order, right for recovery, suit for specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the other Parties from committing any violation or to enforce the performance of the covenants, representations and warranties and obligations contained in this Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies that the Parties may have at law or in equity, including without limitation a right for damages.

15. SURVIVAL

Any provision of or obligation under this Agreement that contemplates performance or observance subsequent to any termination or expiration of this Agreement or which by their nature survive termination shall survive any such termination or expiration, and shall continue in full force and effect.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the	Signed, Sealed and Delivered by the
______________________________	______________________________
(Name & Designation) for and on behalf of	(Name & Designation) for and on behalf of
_________ , One Part (the Bidder)	NABARD, One Part (the Purchaser)

Witness	Witness
1.________________	1.______________________
2.________________	2.______________________

16.ANNEXURE XVI – SLA

SERVICE LEVEL AGREEMENT

FOR

IT SERVICES MANAGEMENT

This SERVICE LEVEL AGREEMENT, made on this __________(day) of _________, 2022 (hereinafter referred to as the "**SLA/Agreement**")

BY AND BETWEEN:

National Bank for Agriculture and Rural Development, a body corporate established under the Act of Parliament i.e., National Bank for Agriculture and Rural Development Act, 1981, having its Head Office at Plot No. C-24, Block G, Bandra Kurla Complex, Bandra (East), Mumbai – 400051 represented herein by its Authorised Representative Shri __________________, (Name, Designation & Department) (hereinafter referred to as "NABARD" which term shall, unless it be repugnant to the context or meaning thereof, be deemed to include and mean its successors, assigns) of the FIRST PART;

AND

__________________________________, a __________________incorporated under the (________________)and having its registered office at ____________________________, together with its Affiliates and represented herein by its Authorised Signatory, (Shri _________________, (name, designation & vertical or division, etc.) hereinafter referred to as the "ITSM Service Provider" , which term shall, unless it be repugnant to the context or meaning thereof, be deemed to include and mean its successors and permitted assigns) of the OTHER PART.

As the context may require, the ITSM Service Provider and NABARD shall, collectively hereinafter be referred to as "Parties" and individually as "Party".

WHEREAS:

6. NABARD is engaged in the business of providing and regulating credit and other facilities for the promotion and development of economic activities in rural areas with a view to promoting integrated rural development and securing prosperity of rural areas, and for matters connected therewith or incidental thereto.

7. The ITSM Service Provider is engaged in the business of ----------------------

8. NABARD had issued a Request for Proposal ("**RFP**") vide Ref No.------ dated-------- for provision of IT Management Services, and had selected the ITSM Service Provider as the successful bidder as per the terms of the RFP.

9. Accordingly, Parties have entered into an agreement on or about the date hereof for the provisions of IT Services Management ("**Principal Agreement**").

10. Pursuant to the Principal Agreement, the ITSM Service Provider agrees to provide Support Services (as defined hereinafter) in relation to IT Services Management to NABARD.

11. The Parties have now decided to enter into this Agreement to record the terms and conditions which will govern the Support Services rendered by the ITSM Service Provider to NABARD during the Term (as defined hereinafter).

NOW THEREFORE, in consideration of the mutual agreements, covenants, representations and warranties set forth in the Agreement, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, the Parties hereby agree as follows:

1. DEFINITIONS

The terms used but not defined in this Agreement shall have the meaning given to such terms in the Agreement. The following terms shall have the meanings assigned to them herein below:

"Application Development" means any tools developed on the specific needs of NABARD for any internal or external use;

"**Affiliate**" of either Party means a person or entity, directly or indirectly, Controlling, Controlled by, or under common Control with such Party;

"**Agreement**" means this Service Level Agreement together with the Recitals, Schedules and Annexures hereto, as amended, modified or supplemented from time to time, in accordance with the terms herein;

"**Background Intellectual Property**" means Intellectual Property owned or controlled by a Party, including Intellectual Property developed prior to or independently of this Agreement, which the Party determines, in its sole discretion, to make available for the carrying out of the Support Services and includes Intellectual Property licensed to or acquired by the Parties from time to time pursuant to this Agreement;

"**Bugs**" means a failure of a software/tool to perform as specified in the applicable product description and/or user's guide and/or installation guide due to defective software distribution media or otherwise;

"**Business Day**" means any day of the week except Saturday, Sunday or any day on which the NABARDs in India are closed for business;

"Consumables" means any items purchased to run the IT operations and make end user productive;

"**Contract Price**" shall mean the total consideration to be paid by NABARD to the ITSM Service Provider as agreed under the Principal Agreement;

"Customization" – means making changes to an Off-the-Shelf software/hardware to meet NABARD's requirements;

"**Discloser**" means the Party disclosing Confidential Information;

"**Effective Date**" shall mean the date of commencement of the Support Services and all other obligations of the ITSM Service Provider hereunder i.e., ---------------;

"Equipment" means any physical appliance that requires installation at the NABARD premises;

"Escalation" means any unresolved queries or service requests in prescribed timeline.

"**Force Majeure**" means occurrence of one or more of the following events which are beyond the reasonable control of the Parties despite having exercised all reasonable care and due diligence, and which are unforeseen, unavoidable or insurmountable, and which arise after the Effective Date and which prevent total or partial performance of this Agreement by either Party. Such events shall include:

a. war (whether declared or not), armed conflict or the serious threat of the same (including but not limited to hostile attack, blockade and military embargo), hostilities, invasion, act of a foreign enemy, extensive military mobilization, civil war, riot, rebellion and revolution, military or usurped power, insurrection, civil commotion or disorder, mob violence, act of civil disobedience;

b. act of terrorism, sabotage or piracy;

c. act of authority whether lawful or unlawful, compliance with any Law or governmental order, rule, regulation or direction, curfew restriction, expropriation, compulsory acquisition, seizure of works, requisition, nationalisation;

d. act of God, plague, epidemic, natural disaster such as but not limited to violent storm, cyclone, typhoon, hurricane, tornado, blizzard, earthquake, nuclear catastrophe, volcanic activity, land slide, tidal wave, tsunami, flood, damage or destruction by lightning, drought or contagious disease;

e. explosion, fire, destruction of facilities, and of any kind of installation, prolonged breakdown of transport, telecommunication or electric current;

f. general labour disturbance such as but not limited to boycott, strike and lock-out, go-slow, occupation of factories and premises; or

g. any other cause beyond the reasonable control of the applicable Party.

Provided that the current ongoing situation regarding COVID-19 and/or lockdowns due to COVID-19 shall not be considered as Force Majeure Event under this Agreement.

“Date of Start of Service” means the start of services after configuration of all tools and migration of existing data after acceptance by NABARD.

“**Intellectual Property**” means all rights resulting from intellectual activity whether capable of protection by statute, common law or in equity and including patents, trademarks, copyright, integrated circuits, trade secrets, know how, design rights, discoveries, ideas, concept notes, business methods, software codes (including source code, object code executable file) and all rights and interests of a like nature including but not limited to methods and techniques, together with any documentation relating to such rights and interests;

"**Materials**" includes source codes, concepts, documents, property, information and the subject matter of any category of Intellectual Property (including all associated documents, data, libraries, tools, and other items and materials necessary or desirable to enable any person or its agents/contractors to fully understand, use, modify and maintain such Intellectual Property);

“**NABARD Data**” means any information or material:

10 disclosed or submitted, directly or indirectly, to the ITSM Service Provider or its Authorised Representative(s) by NABARD in order to perform or in connection with the Support Services;

11 learnt or generated or obtained by the ITSM Service Provider or its Authorised Representative(s) as a result of performing the Support Services; and

12 which shall include information relating to NABARD’s customers, technology, operations, facilities, consumer markets, products, capacities, procedures, security practices, business affairs and other proprietary information,

13 in any media whatsoever (including electronic) and in each case which is in the possession, custody or control of the ITSM Service Provider or and as such data is modified, added to or stored from time to time.

"**Personnel**" shall mean NABARD's employees, executives, board members or individuals engaged in day to day business of NABARD or as may be designated by NABARD;

"**Project**" the design, and implementation of the [*] , by the ITSM Service Provider and maintenance, support and upgradation thereof, pursuant to the Principal Agreement;

"**Recipient**" means the Party receiving Confidential Information;

"Reports" means information from the services in desired format.

"Response Time" means the elapsed time between the receipt of a Support Call and the target time within which ITSM Service Provider Support as verified by a written confirmation to NABARD.

"Resolution Time" means the time between the receipt of a Support Call and the target time within which ITSM Service Provider resolves the issue as verified by a written confirmation to NABARD.

"Scheduled Business Operation Hours" of NABARD is from 9:00 AM to 6:00 PM (IST) from Monday to Friday.

"Service" means any installation, support which makes good of failed service either pre agreed or requested by NABARD

"SLA" – SLA means this Service level Agreement which defines the services provided, the indicators associated with these services, acceptable and unacceptable service levels, liabilities on the part of the Parties and actions to be taken in specific circumstances.

"**Support Services**" means the services to be provided by the ITSM Service Provider to NABARD as set out in Schedule A of this Agreement.

"**Service Levels**" refers to the performance standards required to be complied with by the ITSM Service Provider in relation to providing the Support Services under this Agreement, including the standards as set forth in Schedule A and other standards in relation to the required availability, response times, etc. as may be mutually agreed to between the Parties;

“**Third Party**” means a legal entity, or person(s) that is not a Party to this Agreement, but does not include Affiliates;

“Software” means any tools deployed either Off-the-shelf purchase for the purpose of NABARD by any ITSM Service Provider

“**Trouble Ticket**” means the ticket raised by the Service Desk on receipt of notification by NABARD of any problem;

“**UAT**” means user acceptance testing to ensure that all features as agreed under the Principal Agreement.

“Upgrade” means an improved version of the whole or any part of the System/tool.

“ITSM Service Provider” means any Company or individual who bids for RFP issued by NABARD

2. “INTERPRETATION:

The terms referred to in this Agreement shall, unless defined otherwise or inconsistent with the context or meaning thereof, bear the meanings ascribed to them under the relevant statute / legislation. If there is any conflict or inconsistency between a term in the body of this Agreement and a term in any of the schedules or any other document referred to or otherwise incorporated in this Agreement, the term in the body of this Agreement shall take precedence.

3. SCOPE OF DOCUMENT

This Agreement has been executed in relation to supply & delivery, implementation and support portion of the Project between the Parties. The detailed Service Levels have been set out in this Agreement in the Schedule A.

This Agreement shall ensure the following:

a) Establishment of mutual responsibilities and accountability of the Parties:

b) Definition of each Party's expectations in terms of services provided;

c) Establishment of the relevant performance measurement criteria;

d) Definition of the availability expectations;

e) Definition of the escalation process; and

f) Establishment of single point of contact for trouble reporting;

4. SUPPORT SERVICES

The details of Support Services to be provided by the ITSM Service Provider in relation to the Principal Agreement referred to by NABARD, along with the respective Service Levels, are outlined in Schedule A to this Agreement. The ITSM Service Provider shall provide all other services, functions, responsibilities and tasks that are required for, and incidental to, the proper performance and provision of the Support Services expressly specified in Schedule A.

4.1. Service Levels

1.1.1 The ITSM Service Provider shall comply with the relevant Service Levels set out in Schedule A of this Agreement. In the event, Service Level is not specified for any particular Support Services to be provided under this Agreement, the ITSM Service Provider's performance will be at par with the performance expectation of NABARD with respect to such Support Services.

4.2. Maintaining Service Levels

4.2.1. The ITSM Service Provider shall be responsible for implementing and operating all measurement and monitoring tools and procedures required to measure and report its performance relative to the applicable Service Levels.

4.2.2. The ITSM Service Provider shall submit reports as per Schedule B to NABARD, with such details and in the format, as may be mutually agreed between the Parties, specifying compliance with the Service Levels.

4.2.3. ITSM Service Provider shall provide additional services including advisory and consultancy on such terms and conditions as may be mutually agreed between the Parties as per Schedule A.

5. ANNUAL MAINTENANCE CONTRACT

ITSM Service Provider will provide AMC for the hardware for a period of duration as agreed in Schedule A.

6. AUDIT SERVICES

6.1. If it is desired by NABARD/Reserve Bank of India or its regulators or any regulatory authority of the country, the ITSM Service Provider shall subject themselves to an audit of the systems and processes followed by the ITSM Service Provider for the product supplied to NABARD as also the processes/services, by which, support is being provided to NABARD, including support services, escalation methodologies, change management processes, etc. as per the risk parameters finalized by the NABARD/ such auditors.

6.2. The ITSM Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the NABARD. No Audit or inspection will be allowed till ITSM Service Provider has received at least 5 business days' prior written notice for Audit or inspection conducted by NABARD, while prior notice may not be given for Audit or inspection conducted by Regulatory authority.

6.3. Where any deficiency has been observed during audit of the ITSM Service Provider on the risk parameters finalized by the NABARD or in the certification submitted by the auditors, it is agreed upon by the ITSM Service Provider that it shall correct/ resolve the same within such timelines as prescribed by NABARD. The ITSM Service Provider shall provide certification of the auditor to NABARD regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies were observed

6.4. NABARD reserves the right to call and/or retain any relevant material information/reports including audit or review reports undertaken by the ITSM Service Provider (e.g., financial, internal control and security reviews) and findings made on the ITSM Service Provider in conjunction with the services provided to the NABARD.

7. PERSONNEL AND INSPECTION OF RECORDS

7.1. The ITSM Service Provider shall coordinate with the Authorised Representatives of NABARD, for continuous monitoring and assessment by NABARD of the Support Services provided under this Agreement.

7.2. The ITSM Service Provider shall appoint sufficient number of individuals in order to ensure that the Support Services are provided to NABARD in a proper, timely and efficient manner. The ITSM Service Provider shall provide NABARD with the names of the individuals who shall be involved in carrying out the Support Services and shall obtain approval in writing from NABARD before making any change in such team. The individuals appointed by the ITSM Service Provider shall be those indicated by the ITSM Service Provider under its response to the RFP. Any additional individual shall be appointed subject to prior written approval from NABARD.

7.3. The ITSM Service Provider shall maintain electronic books of accounts, log-books and any other operating records that it may deem necessary in connection with the rendering of Support Services under this Agreement. The ITSM Service Provider shall retain all such electronic books of accounts and operating records relating to the Support Services for a period of 7 (seven) years after the expiry or earlier termination of the Agreement.

7.4. In order to enable NABARD to comply with Applicable Laws, the ITSM Service Provider shall furnish such documents and information, in addition to the books and electronic records maintained by the ITSM Service Provider in terms of Clause 7.3 (Personnel and Inspection of Records) above, as may be requested by NABARD, from time to time, in relation to the Support Services rendered by the ITSM Service Provider under this Agreement at its own cost.

7.5. Upon receipt of advance notice of 3 (three) Business Days from NABARD, whether during the Term or thereafter, the ITSM Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any

Business Day, access its premises to inspect the electronic records maintained by the ITSM Service Provider in relation to the Project.

7.6. If required under Applicable Law, whether during the Term or thereafter, the ITSM Service Provider shall provide access to any Governmental Authority to inspect records, documents, books and accounts of the ITSM Service Provider maintained in relation to the Support Services rendered under this Agreement.

7.7. Manpower hiring – the duties/ obligations, regulatory compliance on the part of the ITSM Service Provider, particularly compliance with respect to the Contract labour Act and other labour laws to be fulfilled by the ITSM Service Provider

8. SUPPORT BY NABARD

8.1. NABARD shall provide ITSM Service Provider with necessary access to NABARD's Personnel and its equipment, only as necessary for provision of Support Services by the ITSM Service Provider. This access includes the ability to dial-in to the equipment on which the Service is required and may also include the ability to obtain the same access to the equipment as those of NABARD's Personnel having the highest privilege or clearance level, strictly as necessary.

8.2. NABARD shall provide supervision, control and management of the Support Services. In addition, NABARD shall implement procedures for the protection of information in the event of errors or malfunction of the equipment.

8.3. NABARD shall document and report all detected errors or malfunctions of any software or programs to the ITSM Service Provider. NABARD shall take all steps necessary to carry out procedures for the rectification of errors or malfunctions within a reasonable time after such procedures have been received from ITSM Service Provider.

8.4. NABARD shall appoint one individual who is knowledgeable in IT operations to serve as primary contact between NABARD and ITSM Service Provider regarding the registry and report of Support calls. The names of the said person shall be promptly intimated to ITSM Service Provider. All of NABARD’s Support inquiries shall be initialized through these contacts.

8.5. NABARD shall annually review the financial and operational condition, security practices and control processes, performance during the year of the ITSM Service Provider to re-assess its ability to continue to meet outsourcing obligations in order to ensure its preparedness for business continuity.

9. Change Requests: Any change requests for addition of any new service would have to be first cleared by NABARD. After finalizing the proposed change, a Business Requirement Document (BRD) will be prepared by ITSM Service Provider followed by acceptance by NABARD at mutually agreed cost.

10. PERIODIC REVIEW PROCESS

This SLA is an operational document and will be periodically reviewed and changed when the following events occur:

8 The environment has changed

9 The customer's expectations or needs have changed

10 Workloads have changed

11 Better metrics, measurement tools and processes have evolved

The SLA will be reviewed as deemed necessary. Contents of this document may be amended as and when required, provided mutual agreement is obtained and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

11. EXCLUSIONS

The Parties agree that the Support services will be provided only on the OEM Licensed products and services thereof and ITSM Service Provider shall not support software that is altered or modified independently by NABARD, or any combination of any with other services, which are not covered under the SLA Agreement.

11.1. Support by ITSM Service Provider shall not include, by default but may provide at additional cost, if solicited by NABARD.

11.1.1. the correction of any error, malfunction or fault in the Scope due to any accident or disaster affecting the system on which the System is located.

11.1.2. the correction of any error due to input error from any other software that is/has been interfaced with the Licensed Software.

12. ADDITIONAL SERVICES

12.1. NABARD regularly undertakes periodic checks and VAPT exercises to identify any vulnerabilities in the system. The ITSM Service Provider shall make suitable changes as per the recommendations emerging from VAPTs emerging within the contract period. The vulnerabilities so identified may be fixed by the ITSM Service Provider within the predefined timeline as follows:

12.1.1. All Critical & High category Vulnerabilities – To be fixed at the earliest with highest priority and within 3 days of informing.

12.1.2. All Medium Category Vulnerabilities – Within 7 days of informing

12.1.3. All Other category vulnerabilities – Within 10 days of informing

13. INTELLECTUAL PROPERTY OWNERSHIP

Each Party agrees that it will not have any ownership claim in the other Party's Background Intellectual Property; and grants the other Party and the Third-Party sub-contractor appointed in terms of Clause (Appointment of Sub-contractors), a non-exclusive, royalty-free license for the use of any Background Intellectual Property made available by the granting Party for the purpose of carrying out the Support Services.

14. CONFIDENTIALITY

a. All data captured and reported by ITSM Service Provider to the NABARD in connection with terms of this agreement shall be deemed to be "Confidential Information" for the purpose of this clause and cannot be disclosed by ITSM Service Provider without written consent of NABARD. Likewise, any information provided by NABARD in terms of this agreement shall also be deemed to be 'Confidential Information' for the purpose of this clause. Use of the confidential information for any other purpose is restricted under this agreement. In case of termination of the agreement the confidential information obtained in material form (except for data captured and supplied to NABARD) should be returned back to the other party. Likewise, the data captured by ITSM Service Provider and retained by ITSM Service Provider is purely for providing service and based on the agreement entered into with the NABARD. The data will be confidential and will not be used for any other purpose. All data captured and obtained by ITSM Service Provider will be property of the NABARD. The Provision of Confidential Information shall survive termination or expiration on this agreement.

b. ITSM Service Provider shall establish and maintain such security measures and procedures as are reasonably practicable to provide for the safe custody of NABARD's information and data in its possession and to prevent unauthorized access thereto or use thereof.

c. NABARD or its affiliates will not use any available decoder for decoding the .exe file for the mobile application shared by ITSM Service Provider and use the software code thus obtained for any purpose.

15. SUBCONTRACTING

15.1. ITSM Service Provider may engage the services of sub-contractors to perform any of its duties with the prior written permission of NABARD. Unless otherwise agreed in writing, no sub-contracting of such duties shall relieve ITSM Service Provider of responsibility for their due performance.

15.2. The ITSM Service Provider shall ensure that the sub-contractor is bound by the terms of this Agreement as applicable. A copy of contract details entered between ITSM Service Provider and sub-contractor to be made available by the ITSM Service Provider to NABARD within 30 days of engaging the sub-contractor.

15.3. ITSM Service Provider agrees that it shall not transfer/assign to any of its rights and/or obligations under this agreement to any entity including affiliates without the prior written permission from NABARD.

15.4. If the parties undergo a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this agreement shall be considered to be transferred to the new entity and such an act shall not affect the rights and obligations under this Agreement.

15.5. NABARD, including its' auditors and regulators, shall have the right to review the books and process of the activities subcontracted to another ITSM Service Provider.

15.6. The ITSM Service Provider shall ensure that all persons subcontracted in rendering services under the agreement have undergone necessary police verification, background checks and other due diligence to examine their antecedents and ensure their suitability for such engagement. The ITSM Service Provider shall retain the records of such verification and shall produce the same to the NABARD as and when requested.

16. LIMITATION OF LIABILITY

16.1. ITSM Service Provider liability to meet the SLAs is limited to 10% cost of agreement during the year of total cost of duration of the service period in which the liability event occurred.

16.2. Notwithstanding anything to the contrary contained anywhere in this Agreement, NABARD shall not be liable to the ITSM Service Provider for any special, consequential, incidental, exemplary, punitive, or indirect damages arising from, relating to, or in connection with this Agreement or any Schedules, Annexures or attachments hereto including, without limitation to, any damages resulting from loss of profits, loss of savings, loss of business, loss of use, or loss of data, arising out of or in connection with this Agreement or of any other obligations relating to this Agreement, whether or not the Party has foreseen or been advised of the possibility of such damages as well as for costs of procurement of substitute services by anyone.

17. REPRESENTATIONS, WARRANTIES AND COVENANTS

ITSM Service Provider hereby represents and warrants to NABARD that:

i. it is duly organized and validly existing under the laws of the jurisdiction of its incorporation or organisation;

ii. it has taken all necessary actions, corporate or otherwise, as applicable to it to authorize or permit the execution, delivery and performance of this Agreement and the transactions contemplated hereunder, and this Agreement when executed and delivered by it is a valid and binding obligation of such Party enforceable in accordance with its terms;

iii. neither the execution, delivery and performance of this Agreement, nor the performance of the transactions contemplated in the Agreement by it, will (i) constitute a breach or violation of its charter documents, (ii) conflict with or constitute (with or without the passage of time or the giving of notice) a default under or breach of performance of any obligation, agreement or condition that is applicable to it, (iii) contravene any provision of any Law applicable to it, or (iv) require the consent of any Third Party, including any Governmental Authority, by it other than as set out in this Agreement;

iv. there are no claims, investigations or proceedings before any court, tribunal or Governmental Authority in progress or pending against or relating to it, which could reasonably be expected to prevent it from fulfilling its obligations set out in this Agreement; and

v. it is not bankrupt or insolvent under the Applicable Laws of its jurisdiction and there are no insolvency proceedings of any character, including without limitation, bankruptcy, receivership, reorganization, composition or arrangement with creditors, voluntary or involuntary, affecting it, or is pending or, to the best of its knowledge, threatened in writing, and it has not made any assignment for the benefit of creditors or taken any action in contemplation of, or which would constitute the basis for, the institution of such insolvency proceedings.

vi. ITSM Service Provider shall provide the Support Services in accordance with the generally accepted industry standards and practices relating to such Support Services and in accordance with requirements specified by NABARD in writing;

vii. the ITSM Service Provider has the requisite infrastructure, facilities and systems, including adequate skill, know-how, and manpower to fulfil its obligations under this Agreement on its own and shall undertake all Support Services and obligations under this Agreement on a first priority basis;

viii. ITSM Service Provider shall exercise highest standards of skill, care, and due diligence in performance of its Support Services and obligations under this Agreement;

ix. ITSM Service Provider has adequate insurance, risk management systems, contingency plans and backup system in place to ensure that it may continue to provide uninterrupted performance of Support Services under this Agreement consistent with the standards agreed hereto;

x. The ITSM Service Provider shall provide Support Services in accordance with the specifications set out under this Agreement;

xi. ITSM Service Provider will not violate the Intellectual Property Rights of Third Parties whilst providing the Support Services;

xii. the ITSM Service Provider shall provide Support Services in the premises of NABARD or in an enclosed environment wherein no third party or any employees of the ITSM Service Provider will have access to such premises. Only such personnel/ Third party sub-contractors (as per Clause 15) of the ITSM Service Provider who are working to or engaged for providing the Support Services under this Agreement between the ITSM Service Provider and NABARD shall have the restricted access to such enclosed environment.

xiii. the ITSM Service Provider shall ensure that the employees of the ITSM Service Provider / Third Party sub-contractors who are engaged in providing the Support Services under this Agreement shall have executed/ execute such confidentiality documents as may be required by NABARD and shall have confidentiality obligations not lesser than those prescribed under this Agreement.

xiv. The ITSM Service Provider shall be fully and completely responsible and liable for all acts, omissions, liabilities undertaken by personnel employed / engaged by the ITSM Service Provider and shall be solely responsible for any and all claims, payments and benefits payable to such personnel employed by the ITSM Service Provider.

xv. The ITSM Service Provider further undertakes to exercise all due diligence with regard to and shall maintain strict controls and physical and digital safeguards in connection with the Support Services.

xvi. any material, codes, applications, front ends, etc created, developed or being used for providing the Support Services under this Agreement shall not be shared with or shown to or discussed with any other entity whatsoever, for any purpose including any development, sales pitch, demonstration or publicity or as examples or otherwise.

xvii. no representation or warranty by it contained herein or in any other document furnished by it to NABARD or to any government instrumentality in relation to the Support Services contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading.

xviii. no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or Personnel of NABARD in connection therewith.

xix. The ITSM Service Provider shall not, whether during or after the Term of this Agreement, make any announcements or statements to any person that are or may be derogatory, defamatory or prejudicial to NABARD, or any of its Affiliates, directors, Personnel, officers, agents or advisors, in any manner.

xx. Appropriately qualified personnel appointed by the ITSM Service Provider shall perform Support Services as listed in Schedule A with due care and diligence and to such high standards of quality as it is reasonable for NABARD to expect in all the circumstances post the expiry of this Agreement.

18. NOTICES

Any notice or other information required or authorized to serve under these SLA shall be in writing, in English language, to be delivered by hand, email, courier or registered post. In case of post or courier, any notice shall be deemed to have been given on the seventh day after the envelope containing the notice was posted**.** The proof that the notice was properly addressed and is not returned to the sender shall be sufficient evidence that the notice or information has been duly given. Either party may change its address, telephone number or email-ID for notification purposes by giving the other party fifteen (15) days' notice of new address, telephone number or email id and date upon which it will become effective.

All communications will be addressed as follows (unless changed by written notice):

Address of NABARD	Address of ITSM Service Provider
Name & Designation:	Name & Designation:
Postal Address/ Office Address:	Postal Address/ Office Address:
Contact No.	Contact No.
Copy Sent to:	Copy Sent to:

19. INDEMNIFICATION

19.1. ITSM Service Provider shall indemnify and agrees to defend and to keep NABARD and its Affiliates and agents, officers, directors, employees successors and permitted assigns indemnified, from any and all Losses suffered arising from, or in connection with, any of the following:

i. the non-performance and non-observance of any of the terms and conditions of this Agreement by the ITSM Service Provider;

ii. acts or omissions of the ITSM Service Provider which amount to negligence or wilful misconduct;

iii. any infringement or alleged infringement by the ITSM Service Provider of a Third Party's Intellectual Property;

iv. any infringement or alleged infringement by the ITSM Service Provider of NABARD's Intellectual Property and/or Material

v. failure by the ITSM Service Provider to fulfil its obligations under any applicable Law.

19.2. The ITSM Service Provider shall, at his own expense, defend and indemnify NABARD against any Losses in respect of any damages or compensation payable in relation to any non-compliance with Applicable Law including (i) non-payment of wages, salaries, remuneration, compensation or the like and (ii) any Losses arising out of or in relation to any accident or injury sustained or suffered by the ITSM Service Provider's workmen, contractors, sub- contractors, ITSM Service Provider s, agent(s), employed/ engaged otherwise working for the ITSM Service Provider or by any other third party resulting from or by any action, omission, or operation conducted by or on behalf of the ITSM Service Provider.

19.3. The rights of NABARD pursuant to this Clause (Indemnification) shall be in addition to and not exclusive of, and shall be without prejudice to, any other rights and remedies available to NABARD at equity or Law including the right to seek specific performance, rescission, restitution or other injunctive relief, none of which rights or remedies shall be affected or diminished thereby.

20. TERM AND TERMINATION

20.1. Term

This Agreement shall commence on and from the Date of start of service and shall remain valid until the subsistence of the Principal Agreement (including all renewals thereof) ("**Term**"), unless terminated earlier in accordance with Clause 21.2.

20.2 Termination

20.2.1. Order Cancellation/ Termination of Contract

NABARD reserves its right to cancel the entire/ unexecuted part of Purchase Order at any time by without assigning appropriate reasons in the event of one or more of the following conditions:

a. Delay in Implementation of the Project beyond the specified periods for reasons solely ascribed to the ITSM Service Provider.

b. Serious discrepancies noted in the implementation of the project.

c. Breaches in the terms and conditions of the Purchase Order.

d. Project adversely affecting the Core Systems or Core Business of the NABARD and the normal functioning of the Offices of NABARD.

e. If ITSM Service Provider fails to upgrade any or all of the critical hardware /software within the period(s) specified in the Contract or within any extension thereof granted by the NABARD.

f. If ITSM Service Provider fails to perform any other obligation(s) under the Contract.

g. If ITSM Service Provider is not providing after sales and maintenance services and the calls are not attended for three or more occasions, NABARD is at liberty to terminate the Contract by giving 30 days' 'Notice'. If ITSM Service Provider provides remedy within 30 days of termination notice, NABARD may reconsider its decision of termination.

h. In addition to the cancellation of purchase order, NABARD reserves its right to invoke the Performance Bank Guarantee given by the ITSM Service Provider after giving notice.

i. Termination in all circumstances will mean a proper transition with data transfer in a readable format along with all knowledge documents. Transition to take within a month unless extended by mutual consent.

j. NABARD, without prejudice to any other remedy for breach of contract, by giving 30 days' written notice of default sent to ITSM Service Provider and if ITSM Service Provider fails to cure the default within the notice period, may terminate this Contract in whole or in part.

20.2.2. EFFECT OF TERMINATION

a. ITSM Service Provider agrees that it shall not be relieved of its obligations under the Reverse Transition Mechanism notwithstanding the termination of the Contract/assignment. Reverse Transition Mechanism would typically include service and tasks that are required to be performed /rendered by ITSM Service Provider to NABARD or its assignee to ensure smooth handover and transitioning of NABARD's deliverables and maintenance. The reverse transition will be for the period of 3 months post the notice period.

b. Same terms (including payment terms) which were applicable during the term of the contract should be applicable for revers transition services.

c. ITSM Service Provider agrees that after completion of the Term or upon earlier termination of the Contract/assignment ITSM Service Provider shall, if required by NABARD, continue to provide services to the NABARD at no less favorable terms than those contained in RFP/Agreement. In case NABARD wants to continue with the ITSM Service Provider's service after the completion of this contract then ITSM Service Provider shall offer the same or better terms to NABARD. Unless mutually agreed, the rates shall remain firm.

d. NABARD shall make such prorated payment for services rendered by ITSM Service Provider and accepted by NABARD at the sole discretion of NABARD in the event of termination, provided that ITSM Service Provider is in compliance with its obligations till such date. However, no payment for "costs incurred or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to ITSM Service Provider.

e. Notwithstanding the termination or expiry of this Agreement, all rights granted to NABARD pursuant to this Agreement shall survive.

f. Each Party shall:

1. promptly, at the other Party's sole option and request, return to the requesting Party or destroy (and certify in writing to such destruction) any and all Confidential Information of the requesting Party, whether in written or electronic form, and neither Party shall retain any copies, extracts, derivatives, or other reproductions of the Confidential Information of the requesting Party (in whole or in part) in any form whatsoever;

2. take reasonable steps to assure that any and all documents, memoranda, notes, and other writings or electronic records prepared or created by the requesting Party, which include or reflect the Confidential Information of the requesting Party, are destroyed.

20.2.3. Termination of this Agreement (except as otherwise agreed to by the Parties) shall not release any Party hereto from any liability or obligation in respect of any matters, undertakings or conditions which shall have been done, observed or performed by that Party prior to such termination or which, at the said time has already accrued to the other Party. However, nothing herein shall affect, or be construed to operate as a waiver of, the right of any Party hereto aggrieved by any breach of this Agreement, to compensation for any injury or damages resulting therefrom which has occurred either before or after such termination.

21. DISPUTE RESOLUTION, GOVERNING LAW AND JURISDICTION

a. This Agreement shall be governed by the laws of India.

b. Any dispute, difference or claim arising out of or in connection with the Agreement which is not resolved amicably shall be decided in accordance with the dispute resolution procedure as set out in the RFP.

c. All disputes and differences of any kind whatsoever, arising out of or in connection with this Agreement or in the discharge of any obligation arising under this Agreement (Whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Agreement) shall be resolved amicably by Parties. Each Party shall select / appoint 1 (one) senior representative. Such discussions towards amicable settlement of the dispute shall be undertaken for a period of 30 days from the date of appointment of both the respective senior representatives ("Settlement Period").

d. In case of failure to resolve the disputes and differences amicably within 30 days of the receipt of notice by the other party, then such unsettled dispute or difference shall be referred to arbitration by sole arbitrator mutually agreed in accordance with the Arbitration and Conciliation Act, 1996.

e. The seat & venue of the same shall be in Mumbai (as agreed in RFP)

f. All disputes arising out of or in any way connected with this Agreement shall be deemed to have arisen at Mumbai only and Courts in Mumbai only shall have jurisdiction to determine the same.

g. The language of the proceedings shall be in English.

h. Notwithstanding anything in the contrary set forth in this Agreement, each Party shall be entitled to seek urgent interim relief in any court of competent jurisdiction

i. Any notice given by one party to the other pursuant to this Contract shall be sent to the other party in writing or by fax and confirmed in writing to the other party's specified address. The same has to be acknowledged by the receiver in writing.

- A notice shall be effective when delivered or on the notice's effective date, whichever is later.

- For the purpose of all notices, the following shall be the current address:

The Chief General Manager
National Bank for Agriculture and Rural Development
____
____
____

22. INDEPENDENT CONTRACTOR

This Agreement does not set up or create an employer/employee relationship, partnership of any kind, an association or trust between the Parties, each Party being individually responsible only for its obligations as set out in this Agreement. Parties agree that their relationship is one of independent contractors. Neither Party is authorised or empowered to act as agent for the other for any purpose and neither Party shall on behalf of the other enter into any contract, warranty or representation as to any matter. Neither Party shall be bound by the acts or conduct of the other. Employees/workmen of neither Party shall be construed or treated as the workmen/employees of the other Party or place any obligation or liability in respect of any such workmen/employee upon the other Party, including without limitation, worker's compensation, disability insurance, leave or sick pay.

23. FEES

1.2 **The ITSM Service Provider agrees and acknowledges that the amounts paid under the Principal Agreement shall be the full and final consideration for the Support Services rendered by the ITSM Service Provider under this Agreement and the ITSM Service Provider shall not be entitled to any additional amounts.**

24. FORCE MAJEURE

a. No Party shall be liable for any default or delay in the performance of its obligations under this Agreement, if and to the extent the default or delay is caused, directly or indirectly, by Force Majeure and provided that the non-performing Party could not have been prevented such default or delay.

b. The affected Party shall provide notice of non-performance due to Force Majeure to the other Party within 24 hours after the start of such non-performance (or, if providing notice within such time frame is not commercially practicable due to Force Majeure, then as soon as possible thereafter) and such non-performance will be excused for the period such Force Majeure Event causes such non-performance; provided that if NABARD determines it is commercially or technically infeasible to cure the Force Majeure and so notifies the ITSM Service Provider , then NABARD may terminate this Agreement effective immediately upon delivery of notice of termination to the ITSM Service Provider .

c. Provided that the current ongoing situation regarding COVID-19 and/or lockdown due to Covid-19 shall not be considered as Force Majeure Event under this Agreement.

25. LIQUIDATED DAMAGES

a. NABARD shall be entitled to recover liquidated damages as set out in Schedule A from the ITSM Service Provider for breach of Service Levels.

b. Except as otherwise specified under Schedule A, if the ITSM Service Provider fails to deliver any Support Services or meet any Service Levels under this Agreement, NABARD shall be entitled to liquidated damages of a sum equivalent to 0.5% percent per week or part thereof of the unperformed services subject to maximum of 10% of the unperformed services for that particular location. In case of undue delay beyond a period of 15 days unless otherwise waived by NABARD, NABARD at its discretion may consider the delay as a ground for termination of the Agreement.

c. NABARD reserves the right to impose / waive any such liquidated damages. Parties agree that the liquidated damages constitute a genuine pre-estimate of the damages, losses, likely to be suffered by NABARD in the event of breach by the ITSM Service Provider of the terms hereof.

d. NABARD may without prejudice to its right to effect recovery by any other method, deduct the amount of penalty from any money belonging to the ITSM Service Provider in its hands (which includes NABARD'S right to claim such amount against the ITSM Service Provider's bank guarantee under the Principal Agreement) or which may become due to the ITSM Service Provider. Any such recovery of penalty shall not in any way relieve the ITSM Service Provider from any of its obligations to complete the Support Services or from any other obligations and liabilities under this Agreement.

26. MISCELLANEOUS

a. This agreement shall be effective for a period of .... years from .... to .... ("Term") unless terminated as per the clause provided in this agreement.

b. All the terms and conditions stipulated in the RFP .... dated ....regarding .... are considered as part and parcel of this agreement.

c. Any provision in this Agreement may be amended or waived if, and only if such amendment or waiver is in writing and is signed by both the parties to this Agreement; in the case of an amendment by each party, or in the case of waiver by the Party against whom the waiver is to be effective.

d. Either party or its employees and representatives shall not use the name and/or trademark/logo of the other party in any sales or marketing publication or advertisement, or in any other manner without the prior written consent of the other party.

e. Terms of Payment: In consideration of the Services and subject to the provisions of the RFP and this Agreement, the NABARD shall pay the amounts in accordance with the Terms of Payment Schedule of the Purchase Order.

f. ITSM Service Provider shall provide, if asked, copy of necessary valid compliance certificates with details of validity period from time to time as well as and when there is a change.

g. ITSM Service Provider will not release any factual information concerning these SLAs Agreement to any person/news media without prior permission of NABARD.

THIS AGREEMENT shall be executed in two numbers, one will be kept with NABARD and the other with ___________ **(Service Provider).**

IN WITNESS WHEREOF, the parties hereto, through their duly authorized officers have caused this Agreement to be duly executed and delivered as of the date first above written.

NABARD________________	**(Name of Service Provider)_________________**
Signature:_______________	Signature:___________________________
Name :	Name:
Title :	Title :
Place :	Place :
Date :	Date :

WITNESS	**WITNESS**
Signature : ____________________	**Signature_________________________**
Name :	Name :
Address :	Address :

SCHEDULE - A

Project Scope of Work

IT Service Management

a. AMC for IT assets and Peripherals

b. Desktop Management using the centrally managed tool

c. Inventory Management using tool

- Configuration management (system and devices configuration at DC/DR/HO/RO/TE) and any other location prescribed by Bank.
- Ticket logging for warranty support of all devices.

d. Patch Management using tool

e. Domain Service Management (Active Directory, LDAP)

f. File Services Management

g. Storage Management

- Storage Management (allocation, monitoring, troubleshooting)

h. Backup Management

- Backup and Storage management (Arcserve & HPDP)

i. Data Center and Server Management

- Server management (Maintain server log book, install, update, troubleshoot, tuning, monitor, auto alert, SSL installation, certificate based access), JBOSS Support, all native OS services of windows, linux, AIX, webservers
- HCI (Hyper Converged Infrastructure), SDDC maintenance and management of clustered servers.

j. Network Management Services

- Network Management and Automation Solution, Support and co-ordination for IFTAS cloud

k. IT Security Management

- Networking, Firewall, UTM, NAC, Wi-Fi, ILL, MPLS, IFTAS and SDWAN maintenance and management. (e.g. Juniper, Fortinet, Forcepoint, checkpoint, sonicwall, etc)

l. Database Administration

- Database Management (install, update, fine tuning, replication, recovery, backup & restore, monitoring, auto alert)

m. Vendor Management

n. HelpDesk and Service Desk Management

- Ticketing processes (ticket logging, classifying, assigning, resolving, escalating), helpdesk and services.

o. General

- Process flow Management of all ITSM verticals.
- Capacity Management (Assigning, troubleshooting, alerting)

2. **Scope involves the provisioning and management of mentioned ITSM requirements, based on the Bank's requirement as stated in the RFP.**

2.1 NABARD would like to avail these services in a managed service model through a single ITSM Service Provider. All necessary tools, software's (All Licenses should be in name of NABARD) necessary for the administration and management of all the service components should be provided as mentioned in clause 4.1.1.

2.2 All the service monitoring and management tools must be deployed on-premises. Monitoring and Management Tools should be available to both onsite and offsite teams for delivery of these services.

2.3 Web based asset and inventory management tools with access for DIT users and management.

2.4 Option of API based integration with other applications should be available in asset and inventory management tool.

2.5 ITSM service provider should maintain onscreen display panel of ticketing and all devices/infra services dashboard.

2.6 The activities like capacity planning, architecture re-designing (for DC /DR/HO/RO and Network) etc. must also be provided for all the above services.

2.7 The scope of ITSM Service Provider contains support for the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches:

- Firmware/BIOS Upgrades / up to date patching,
- Faulty Parts replacement,

- Hardware System monitoring,
- Troubleshooting & Performance Tuning,
- Operating System Upgrades, antivirus and software upgrades,
- Upgrades of supplied software, all commonly used softwares
- Advisories on software upgrades & vulnerabilities
- DR Drills operations based on SOPs of Nabard.
- OS Administration & patching as per OEM guidelines
- VAPT Compliance/Audit /Review as per Bank's requirement /Statuary guidelines
- Any support required to make system & solution up and running as per SLA.

2.8 The ITSM Service Provider should keep the bank explicitly informed about the end of support dates of the related products/hardware and should ensure support during the warranty and AMC period.

2.9 The ITSM Service Provider should provide the complete documentation including technical, operations, user manual, design documents, process documents, technical manuals, functional specification, system configuration documents, system/database administrative documents, debugging/ diagnostics documents, test procedures etc.

2.10 The ITSM Service Provider shall formulate/ supply/share all kinds of procedures/ documents upon any level or version changes, clarification, corrections and modifications in the above-mentioned documents on each incident of change.

2.11 ITSM Service Provider requires to install and configure Comprehensive Monitoring of End-to-End IT Services (Network, Server, Storage, Appliance, Database and Applications across all locations of the Bank)

2.12 The ITSM Service Provider shall implement Active Directory Certificate Services (AD CS) to create Public key infrastructure in the bank environment to underpin identity and other security functionality on windows domain so that it can create, validate and revoke public key certificates for internal uses of the organization. The ITSM Service Provider shall do end to end management of Active Directory System of the Bank for all services.

2.13 The ITSM Service Provider shall ensure end to end completion of all activities initiated as part of the project. The ITSM Service Provider shall coordinate with other stakeholders also for completion of activity.

2.14 The ITSM Service Provider shall migrate all the data from existing ITSM and IT Asset Management tools to new tool.

2.15 The ITSM Service Provider shall provide the details of all tools/softwares they will be using for ITSM service management, ticketing, monitoring, inventory management, patch management, os installation, desktop support tool etc.

2.16 The ITSM Service Provider shall provide user logins for DIT staffs on all tools/software used for ticketing, monitoring, inventory management, etc.

2.17 The ITSM Service Provider will have to handover the system in 100% working condition on termination or at the end of the contract. Any breakdown call that has been reported before termination of the contract shall have to be corrected by the ITSM Service Provider before handing over to Bank.

2.18 The Bank can terminate the contract with Service Provider and discontinue the same due to performance issues by giving 90 days' notice.

2.19 Contract can be extended at the discretion of the bank at the same rate for last service year after the expiry of the contract period.

2.20 The Bank, at its sole discretion, will enter into AMC for IT assets.

2.21 Bank at its discretion can terminate the contract in whole or as part thereof with the ITSM Service Provider and discontinue the same without citing any reason by giving 90 days' notice or applicable amount, on a pro-rata basis.

2.22 Submission of periodical reports on the performance of the equipment's and its reviews. Preparation and submission of other MIS related work assigned by the Bank.

2.23 A suitable mechanism for setting priority for critical events on the basis of service impact and user groups (VIP users) should also be provided for all these services.

2.24 The ITSM Service Provider shall ensure regular backup as per the backup policies of NABARD and its restoration as and when required by the bank with appropriate permissions. Proper check of restorability of backup media needs to be carried out periodically as defined by the bank.

2.25 Preparation of SOP of all verticals for all existing and new services from the day 1 (one) of service contract.

2.26 Periodic Review all SOP

2.27 ITSM service provider should ensure pay the higher minimum wages between central and states governments and other statutory guidelines as applicable during the period of contract. Service provider should submit necessary certificates to NABARD in this regard.

2.28 Manage operations for all upcoming cyber security solutions i.e. IAM (Identity and Access Management), DAM (Database access management), Brand Monitoring Solution, DNS security, Patch Management, Vulnerability Management, DLP(Data Leak Prevention), security and any other solution.

3. Detailed Requirements

3.1. Annual Maintenance Contract (AMC)

3.1.1. As and when NABARD acquires new IT asset(s) after the start of this contract, coordination and timely closure of warranty and extended warranty related requirements for all IT assets. If on expiry of essential warranty/extended warranty, NABARD decides to enter into AMC of assets such as Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanner with ITSM service provider, rate for the same will be determined based on the unit rate already decided for the existing item in AMC.

3.1.2. The type of maintenance will be fully comprehensive on-site including repair /replacement of parts and if not repairable, ITSM will inform NABARD within 7 days. Maintenance Services shall consist of preventive and breakdown maintenance of Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanners.

3.1.3. A rate card will be part of quote based on SOP for attending to complaints within 48 hours for all district/cluster offices of the bank.(Rate card annexure).

3.1.4. If 'End of Service Life' (as mutually agreed between NABARD and the Service Provider) of an asset falls in between any quarter during contract period, Service Provider will intimate NABARD at least 90 days in advance for replacement of the same. However, Service provider shall continue to provide AMC and ITSM support for these items till NABARD replaces them with new items.

3.1.5. At any stage of the contract, NABARD reserves the right to terminate the AMC for any of the item(s), with due prior notice of 30 days to the service provider. Service provider shall raise invoices for all the subsequent quarters after deducting the AMC charges for the items taken out of AMC.

3.1.6. The current timings for providing AMC services are given below. It is possible that these timings may change in future, but the total working hours will be 9 hours on weekdays.

Working Day	**Time From**	**Time To**
Monday to Friday	9.00 am	6.00 pm (or as required)
Saturday/Sunday/Holidays	As required	As required*

*At no additional cost

Online attendance portal access should be provided by ITSM service provider to DIT management for all their staff including subcontractors along with daily email of attendance sheet at 9:15 AM.

3.1.7. The service segment can be split, if need be, into critical and non-critical services for the purpose of round-the clock on-site monitor.

3.1.8. The complete inventory of all the IT Assets / Equipment which are to be managed and services are given in the **Appendix IV**

3.1.9. The Service Provider will have to provide support for all computer hardware, software and network related calls as logged by NABARD. Service Provider will be responsible for troubleshooting and resolution of related calls and report them back to Central Helpdesk.

3.1.10. The Service Provider will undertake to maintain highest service standards as per good industry practice. The Service Provider will arrange for qualified and experienced resident engineers to meet the above-mentioned service levels. For successful implementation and smooth functioning of the operations, personnel with appropriate skills, aptitude and experience would be deputed at NABARD offices. Service Provider shall submit resumes of engineers to be deployed at NABARD. NABARD would have the right to accept / reject the proposed personnel. Also, if any personnel were to quit then handholding would be necessary with suitable replacement with prior notification to NABARD.

3.1.11. The Service Provider will provide on-site maintenance services. Service Provider should provide PC/Printer/Notebook Computer/Networking equipment in case the problem is not resolved within 4 working hours for the concerned user to carry out his day-to-day work from buffer stock of NABARD. ITSM Service Provider shall provide all essential tools, service kit and testing toolkit needed for maintenance of the computer systems at all locations.

3.1.12. The ITSM Service Provider shall conduct preventive maintenance as may be necessary from time to time (minimum twice in a year) to ensure that equipment is in efficient running condition to ensure trouble free functioning.

Preventive maintenance Scope

a. Physical cleaning using blower.
b. Bios updates.
c. OS and antivirus patch updates.
d. Software updates.
e. Inventory update
f. Any other related activity

3.1.13. The ITSM service Provider shall conduct physical verification of assets minimum once in a year or as need arises.

3.2. Desktop Management using the tool

The ITSM Service Provider should be capable of installation, configuration and using the tool and perform the following activities:

3.2.1. Taking control of remote desktops using tool.

3.2.2. Remote Management of Desktops - installation, configuration and troubleshooting of operating system, Anti-virus and all user Applications in the desktops/laptops.

3.2.3. Remote installation of patches

3.2.4. Remote Routine maintenance of PCs (e.g., cleaning up file system debris, defragmenting drives, running malware scans, etc.)

3.2.5. Taking back-up while configuring new systems.

3.2.6. Guide and direct users to relevant desk/department/individuals in case support required is not under scope of deliverables by the ITSM Service Provider and carrying out related activities.

3.2.7. Use latest technology for bulk installation for multiple machine.

3.2.8. Special Note: Desktop management services are required to be provided for IT equipment (i.e. PC/AIO, Printer, Laptop, Scanner, Internet etc.) at the residences of senior executives (CGM/OIC and above) at all locations and KVS, Dadar.

3.3. Inventory Management using tool

The ITSM Service Provider should perform the following activities:

3.3.1. Capable of installation, configuration and using the tool (import of existing data).
3.3.2. Should maintain the Catalog of software and hardware from all major OEMs/Principals and should update the signature for the same on periodic basis. The update periodicity should be as per industry norms.
3.3.3. Managing Configuration Management data base (CMDB).
3.3.4. Initially, complete inventory of all IT assets in the Bank has to be taken up independently with relevant tools and the same has to be shared with the Bank and later on periodicity as decided by bank.
3.3.5. Dashboard to identify the addition and deletion of IT assets in the Bank for custom period.
3.3.6. Capable of Configuration item (CI) identification, planning and controlling configuration changes
3.3.7. Capable of configuration change report generation
3.3.8. The service provider will do the lifecycle management of the licenses including initiation of procurement request, after purchase, allocation, de-allocation, license renewal alert, license pool management.
3.3.9. Software Licenses Tracking & Management - This includes number of licenses for particular software, which NABARD has purchased, how many have been deployed, what is the entitlement etc.
3.3.10. Should support management of multiple licensing models based on User, Machine, IP, Core etc.
3.3.11. And any other related activities.

3.4. Patch Management using the tool

3.4.1. The ITSM service should include a patch management solution that offers all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating systems.
3.4.2. All critical application/software should also be patched as soon as patch/upgrade is available.
3.4.3. Assist, Develop, Manage and Monitor suitable Policies, Procedures and deployment strategy for Patch Management.
3.4.4. Maintain an up-to date plan for deploying and managing patch management.
3.4.5. Install and test patches and updates in Test environment provided by NABARD and after approval roll-out in the client computers
3.4.6. A practical and up-to date roll back plan has to be adopted in case of failures.
3.4.7. Raise Change Management for deployment of patches or updates.

3.4.8. Schedule shutdown of production system and inform users before applying patches, updates to Servers.

3.4.9. Implement patches as per approved deployment strategy.

3.4.10. Follow up and co-ordinate with OEM/ 3rd party support vendors for patch deployment on all devices.

3.4.11. Build a suitable backup and disaster recovery procedure for maintaining 100% availability of the Patch Management Server and resources.

3.4.12. Report on installed and missing patches

3.4.13. Removal of Software and service packs in case of need and roll back of patches and service packs in case of need.

3.4.14. Capability to identify the devices where patches are applied but not yet activated (pending restart).

3.4.15. A quarantine area has to be maintained for isolating the devices that are not patched up/updated with requisite updates.

3.4.16. Able to communicate effectively at all levels of the organization, and with Vendors in written and oral format.

3.4.17. Maintain smooth operation of multi-user computer systems, including coordination with network, software, and system engineers, PC desktop technicians, project managers, end users, and customer and IT management.

3.4.18. Interact, meet, discuss, and troubleshoot issues with Venodrs; evaluate Vendors products, services, and suggestions.

3.4.19. Maintain security audit information in tracker sheet for all patching related activities.

3.4.20. The tracker to be shared with DIT on weekly basis for review.

3.4.21. And carrying out other related activities

3.4.22. Solution should support system architectures.

3.5. Domain Services Management

The ITSM Service Provider should be capable of installation, configuration of solution along with other administrative tasks:

3.5.1. Existing Domain Server and User Admin have to be managed effectively with the help of suitable tools.

3.5.2. The service should include plan, design and set up and upgrade of additional controllers/forest during the contractual period.

3.5.3. Should co-ordinate, guide and assist in integrating any other systems for SSO /2FA and also digital certificate.

3.5.4. Root domain administration (AD & LDAP) by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.

3.5.5. Administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, and providing administrative support for print, file, and directory services.

3.5.6. Periodic reviews of domain level rights and privileges

3.5.7. Periodic AD (Active Directory) data updation and data interlinking with HRMS for auto updation.

3.5.8. AD integration with other applications

3.5.9. Any other related/similar activities.

3.6. File Services Management

A Windows File Server is being used in NABARD with specific usage space for departments and Regional offices. The same setup has to be managed by the ITSM Service Provider. The ITSM Service Provider should support this.

Functionalities of the File Server

A file server provides a central location for storing and sharing files across the network. ITSM Service Provider should be able to perform following roles:

a. Storage management: This console allows administrators to manage shared folders and allows users to access shared folders over the network.

b. Distributed File System (DFS): Provides tools and services for DFS Namespaces and Replication services.

c. DFS Namespaces: Allows user to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears as a single shared folder with a series of subfolders.

d. Replication: Allows to synchronize files/folders on multiple servers across the network.

e. File Search: Fast file search capabilities

f. Indexing service: Allows indexing of files and folders for faster searching.

g. The access to files should be based on User Rights controlled by Domain Services.

h. Selective Syncing of data in fileserver with cloud.

i. The ITSM Service Provider should be capable of installation, configuration, and management of the above stated file server.

j. Replication of the files/folders and capable of handling the File Services Management functionality.

3.7. Storage Management

The ITSM Service Provider should be familiar with setting up, configuration and usage of the prescribed storage management environment and is required to carry out the following activities:

3.7.1. Incident Management

Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.

a. Configuration of SAN whenever a new application is hosted on the SDC. This shall Include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc

- **b.** Monitoring service availability, resource usage
- **c.** Troubleshooting system alerts with knowledge base
- **d.** Network reachability
- **e.** Administer SAN storage arrays and SAN fabrics and Participate in SAN on-call rotation
- **f.** Providing timely compliance to the audit observations related to storage infrastructure as observed during various internal/ external audits
- **g.** Preparation/Revision of Standard Operating Procedure (SOP) document for the Storage Administration.

3.7.2. Problem Management

- **a.** Closure of incidents effectively.
- **b.** Liaise with service providers for escalation and Root cause analysis
- **c.** Preparation of Preventive Maintenance calendar and configuring replication.
- **d.** SAN / NAS access control review.

3.7.3. Performance & Audit Management

- **a.** Monthly / Fortnightly incident analysis.
- **b.** Audit of administrator accounts.
- **c.** Preparation of capacity planning report.

3.7.4. Backup Management (All Servers at DC and DR)

a. Performing backup operations for the servers as per the defined backup strategy.

- **b.** Ensuring proper storage and handling of media to prevent data loss.
- **c.** Conducting restoration drills with sample backed-up data on a quarterly basis to confirm data integrity.
- **d.** Maintaining log sheets of all backups taken at DC, DR and other locations.
- **e.** Implementing best practices on backup.
- **f.** Installation, re-installation, upgrade and patch deployment of the Arcserve, HPDP, etc. in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.
- **g.** Generation and publishing of backup reports periodically
- **h.** Coordinate with the backup tape movement service provider/ courier agency and the identified nodal officer(s) for sending/ receiving tapes. Maintain tape movement logbook at DC & DR.
- **i.** Coordination for maintaining inventory of off-site tapes at respective locations i.e., DC, DR, Head Office etc.

j. Tape/ LTO library management – loading and unloading tapes, etc at DC & DR.
k. Forecasting tape requirements and giving timely indent to concerned team for timely procurement of the new tapes/storage
l. Reporting of failed backups with critical alerts and ensuring that those are restarted and completed successfully within the backup cycle
m. Update/ Maintain Standard Operating Procedure (SOP) documents
n. Regular review of backup process and assist team to manage capacity planning.
o. Weekly movement of tapes between DC and Head Office, Mumbai, Delhi RO and DR site (Preferably on Friday)
p. Insertion of tapes in tape library at DC & DR site
q. Ejection of tapes from tape library at DC & DR site.

3.8 Data Center and Server Management

3.8.1. ITSM Service Provider should be capable of installation, configuration, and usage of the prescribed tool. Additionally, key points of expectations from the personnel are:

a. Regularly monitor and log the state of environmental conditions and power conditions in the Datacenter.
b. Service support at DR is required as and when required.
c. Periodic review arrangements at Data Center(DC&DR) in terms of cooling, power, positioning of racks &other hardware etc. on an annual basis. The SP shall be required to do first such assessment and submit a report thereon within a period of 2 months from the date signing of contract.
d. Coordinate with NABARD and third-party Service Providers to resolve any problems and issues related to the Datacenter & DR Site environment conditions. Power, air-conditioning, UPS, LAN, Servers, racks, fire, water seepage, dust cleanliness, implementing any changes, layout of infrastructure within the Datacenter & DR Site etc.
e. Suggest/Assist NABARD on best practices of the industry which may be required to be implemented in Data Center.
f. Patch management, upgrades to the systems.\
g. Ensure compliance of NABARD IT Security policies and compliance pertaining to Physical Security equipment in the DC.
h. Maintain high server availability through active performance monitoring and low impact, on- demand remote management services for devices present at DC&DR.
i. Installation, Updation configuring, hardening, trouble shooting of system (Hardware, Firmware and software) across all locations of NABARD
j. Mounting and Unmounting of all hardware components and Cabling, labling, tagging.

k. In case of repetitive hardware failure (three times in a period of three months) during warranty and AMC period, ITSM should coordinate to ensure that they are replaced by equivalent new equipment by OEM/Vendor as per SLA between NABARD and OEM/vendor.

l. Capacity planning and life cycle management of servers and other hardware and IT systems.

m. Online tracking and Inventory management of all the hardware devices including spare materials and periodical updation and review of the same

n. Regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.

o. All firewall, critical servers logs to be maintained for a period defined by NABARD.

p. Management of load balancers

3.8.2. Manage Nutanix Virtualized environment and other HCI virtualized environment including ODA and other cloud. The Nutanix (Virtualization) and other HCI equivalent skill set requirements are as below:

a. Knowledge and administration of industry leading virtualization software / technologies.

b. Knowledge of Nutanix virtualization, VM replication, FLOW, LEAP, XPLAY, prism central, etc.

c. Design and develop service virtualization framework.

d. Configure, deploy, monitor and support Nutanix nodes and clusters.

e. Define best practices, processes for service virtualization.

f. Maintain and configure Service Virtualization tool.

g. Troubleshoot the issues.

h. System installation and maintenance of Windows, AIX and Linux systems.

i. Windows, Linux, AIX, Arcserve, HPDP and Nutanix administration.

j. Knowledge of data center operations.

k. Administration of DNS (IPAM), SMTP, FTP, SSH, LDAP, and NFS services.

l. Patch management, upgrades to critical systems.

m. SAN/NAS storage systems knowledge.

n. Hardware, software and network troubleshooting.

o. Understanding of new business initiatives and the implementation of technologies to facilitate them.

p. Manage systems to achieve 24x7 availability.

q. Work closely with the storage, network and development groups to ensure business continuity.

r. Conduct trainings, mentor and coach teams on Service Virtualization

s. Valid Nutanix NCP-MCI-5 certification or higher.

t. Administering/monitoring Nutanix PRISM Console along with Nutanix nodes, clusters, hosted VMs in DC and DR. Further, the SP shall also monitor, upgrade and update Acropolis OS, AHV Hypervisor etc. Work will involve regular creation of VMs, cloning and monitoring performance of each VM. This shall require conducting regular health checkups and submit regular reports on overprovisioned VMs in terms of RAM, memory, cores etc. for the VM and cluster. Perform capacity planning from time to time.

u. Co-ordinating with necessary stakeholders (after due approvals from authority) for allocating appropriate resources and providing technical inputs for best practices wherever necessary for VM creation, cloning and monitoring performance of each VM

v. Regular co-ordination and advisories related to the conduct of DR Drill which take place every quarter.

w. To act as a trusted advisor to customer IT Teams, providing guidance as well as suggesting Nutanix and other VMware best practices.

3.8.3. JBoss Administration:

a. Support for CLMAS Upgrade for NABARD and its subsidiaries and RADP Platform
b. JBoss Installation and JDK configuration
c. JBoss Hardening and Upgrade
d. .ear, .jar, .war file Deployment
e. .jsp file attachment in tmp folder
f. App to Database connectivity configuration
g. Java Heap size changes
h. Port configuration (8080,18080, http and https)
i. Process kill JBoss
j. JBoss Service start / stop
k. Logs monitoring
l. New instance creation
m. Configuration file changes
n. SSL certificate installation
o. Daily Health checkup of JBoss Application Server

3.9. Network Management Services

ITSM Service Provider should be familiar with all the functionalities of Network Management Services and should broadly carry out the following responsibilities:

3.9.1. Monitoring:

a. Bandwidth utilization, end user bandwidth.
b. QoS and traffic shaping requirements/SDWAN management
c. Link latency
d. Uptime of all devices and servers.
e. Port utilization and growth
f. Marry port and patch panel utilization for audits
g. Audit and advice on rack utilization and growth

h. Inform the County of growth requirements for cabling such as network drops or fiber backbone Monitoring of Traffic Pattern over WAN
i. Follow up with Regional Offices for connectivity related issues
j. Monitoring and troubleshooting of L2 /L3 switches.
k. Monitoring Jitter, Latency, Availability, Bandwidth usage
l. Managing existing Firewalls, UTM, and VPN Services.
m. SDWAN monitoring, management and troubleshooting.
n. Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.
o. Managing NAC setup.
p. Managing Wi-Fi setup.
q. SFMS support

3.9.2. Vendor Management:

a. Enforcing SLAs with external networking Vendors.
b. Opening and managing support cases with external networking vendors/ISPs for various issues such as offline connections and SLA violations
c. Maintaining escalation matrix and ensuring the creation escalation matrix wherever required.
d. BGP etc and other NOC related coordination with ISP
e. OEM/SI related coordination for hardware issues.
f. Coordinate with these vendors for support services.
g. Maintain good relations with them on behalf of NABARD.
h. Logging calls, coordination and follow-up with vendors.
i. Escalation of calls to the higher levels at vendor's side in case of requirement.
j. AMC/ Warranty/ Support Tracking
k. Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the vendor will be made separately by NABARD)
l. Management of assets sent for repair.
m. Maintain database of the various vendors with details like contact person. Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with vendors, Coordinate and follow up with the vendors and ensure that necessary spares exchanged.
n. Analyze the performance of the vendors periodically (Quarterly basis or as specified).
o. Keep NABARD updated on the services and performance of these third-party vendors.
p. When a new solution software is introduced, training to users to absorb and leverages the technology for business should be invariably arranged. And other related activities.

3.9.3. Administration:

- **a.** Managing routers, switches, firewalls, load balancers, wireless access points, and any other networking equipment
- **b.** Assigning, allocating, and auditing network ports
- **c.** Assigning and reassigning VLANs
- **d.** Administering QoS policies as needed
- **e.** Administering 802.1X authentication configurations where applicable
- **f.** Firmware, application, controller, and operating system patching and maintenance
- **g.** Maintain, audit, and extend the given IP schema and routing architecture
- **h.** IPv4 with the intention to include IPv6 in the future
- **i.** Maintain, audit, and extend multicast support throughout the network where applicable
- **j.** Any other work assigned from time to time.
- **k.** IS audit related information should be provided by the ITSM Service Provider.
- **l.** Providing GUI based interfaces to readily check MPLS links status and utilization, health status of devices, Application based traffic (QOS) across all the locations ROs/HO

3.9.4. Lifecycle Management:

- **a.** Inform the bank of bandwidth requirement/infrastructure upgrade and upgradation on a quarterly basis.
- **b.** Participate in the identification and purchase of additional or replacement equipment

3.9.5. New Project inclusion:

In case bank is in process of implementing a new project. The requisite change request for successful implementation, management and operational support of the project should be submitted by ITSM Service Provider on request

3.9.6. FMS services for Network at HO/DC

ITSM Service Provider should be familiar with all the above-mentioned functionalities of Network Management Services and should broadly carry out the following responsibilities:

3.9.6.1. Monitoring

- **a.** Monitoring of the main/backup Links and reporting\
- **b.** Monitoring of Bandwidth utilization, latency, packet loss etc.
- **c.** Managing NAC setup.
- **d.** Managing Wi-Fi setup.
- **e.** Monitoring of Traffic Pattern over WAF
- **f.** Follow up with Regional Offices for connectivity related issues

g. Monitoring and troubleshooting of L2 /L3 switches.
h. Monitoring Jitter, Latency, Availability, Bandwidth usage
i. Managing existing Firewalls, UTM, and VPN Services.
j. SDWAN monitoring, management and troubleshooting.
k. Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.

3.9.6.2. Incident Management

a. Call logging and co-ordination with MPLS VPN service provider for restoration of link
b. Co-ordination with MPLS VPN service provider for ensuring backup lnks are made operational in the event of failure of primary and secondary links
c. Follow up with Service Provider to get detailed RFOs/RCA.
d. Prepare the Link wise outages and calculate the SLA Report to enable processing of the Service Provider Invoices
e. Prepare the Detailed payment note for due processing depending on SLAs.

3.9.6.3. Configuration Management

a. Configuration of L2 switches for administration and L3 Switches for VLAN creation / hardening etc.
b. Installation & Upgrade of switches as and when provided by the OEM/SI.
c. Changing configuration based on NABARD requirement and follow-up with MPLS VPN service provider for application of same on all routers.
d. Maintaining / Updating the WAN diagram at all locations/offices in co-ordination with NABARD IT team and Local Service Provider
e. Maintaining complete inventory of network hardware along with interfaces. IP address, Device OS version etc.

3.9.6.4. Reporting

a. Maintenance of daily/Weekly and monthly uptime report.
b. Present monthly performance review report with highlights/lowlights etc.
c. Collection of daily / weekly and monthly uptime/downtime report from MPLS VPN service provider.
d. Verification of daily report with the fault ticket generated by the MPLS VPN Service provider.
e. Cross verification of daily report with weekly and monthly report and calculation of uptime / downtime.
f. Co-ordination with MPLS Service provider for the replacement/up keep
g. Maintenance of defective Networking Hardware/Software (Like Routers. Modems. Switches etc.) and escalation, if necessary.

3.9.6.5. Advisory Services

a. Advisory services for revamping networks and introducing new network devices and services are also needed.
b. Periodic review mechanism should also be introduced for service improvements in this work area.

3.9.7. Onsite Support Engineer's Role for Network Animator tool (But not limited to this),

a. The engineer will perform following L1/L2 tasks in NMS solution with regards to the tools implemented at bank.
b. Perform daily tools health check based on checklist (services, processes, log file for any errors, application disk.
c. Perform all L1 level troubleshooting (Tool Management System Level) and assist Bank's Network Support team for troubleshooting.
d. Perform MACD (Move/Add/Change/Delete) activity such as adding/removing N/W devices, Servers from,
e. Perform Tasks like adding/modifying assignment group members, categories.,
f. Perform L1 level troubleshooting and follow L2 escalation matrix for non-resolved incidents.,
g. Coordinating for for L2 troubleshooting.,
h. Act as coordinator and provide assistance to OEM's remote support teams for troubleshooting/resolving the product,
i. Ensure all Service Requests, Incident and changes are logged and tracked till closure.,
j. Generating out of box reports as and when required by Bank.
k. Analyze network bandwidth report and device utilization to advice NOC team for Bandwidth up-gradation etc.
l. Daily MIS reporting of all the critical links.
m. Log the call with the OEM for critical tools issues,

3.9.8. Onsite Support Engineer's Role for NCCM tool (But not limited to this)

a. Any configuration changes requested by bank for DC/DR or branch devices.
b. Take care of configuration change and roll back as per bank person request.,
c. Do the solution fail over testing on critical devices b/w NLS and DR on weekly basis.,
d. Take back up for all network and security devices on daily basis.,
e. Creating any new configuration/ configuration template/job/tasks etc as and,
f. DC/DR/Branch devices hardening configuration changes as per banks network,
g. Syncing of DC& DR devices on weekly basis.,
h. Monitor the solution intimate banks on any compliance breach & rectify based on bank team request as and when required.,
i. Share compliance report on daily basis.,

j. Inform banks team in case of any alert /error observed in any device configuration and act according to,
k. Failover testing of critical devices on weekly basis as per bank team's request.,
l. Ensure that all backups are happening correctly and need to maintain and submit the checklist on,
m. Prepare and submit day to day activity report on daily basis.,
n. Periodic discovery of all all the network devices & share the list of noncompliance devices and do the required changes to make it compliant only after bank's team permission.,

3.9.9. SDWAN Forcepoint SMC

a. Management of the architecture –documentation of present architecture, BGP peering management with ISP.
b. IP Sec tunneling for various sites and traffic management on the tunnels
c. Routing on various devices at ROs/HO
d. QOS as per Banks requirement
e. Configuration of Any other feature available on SDWAN as required by bank

3.9.10. Wifi controller

a. Definition of levels according to network security
b. Management of Guest access
c. Management of access privileges.

3.9.11. Support services for CCIL, RTGS/NEFT applications and payment infrastructure management:

a. Onsite support for issue-resolution on all working days and as per emergency requirement beyond working days and holidays.
b. Remote support Telephonic / Network
c. Preventive Maintenance and System Health Checks
d. D.R. Drill assistance
e. Upgrade / Version Management
f. Re-installation / Re-location of Systems and Applications
g. License Management (Track and coordinate for validity)
h. CCIL Systems Help Desk Support
i. Single point of contact for
    i. Regulatory Authorities (RBI, IDRBT, CCIL)
    ii. Applications vendor
    iii. Principals (IBM, Microsoft, Cisco etc.)
j. Service Window
k. Trouble shooting and issues management
l. Patch Management (OS and Middleware)

m. Performance Management

n. Configuration of MQ7 on servers.

o. Trouble shooting and issues management

p. Escalation of issues to appropriate vendor

q. Testing of client server connectivity, member to host connectivity and application level testing.

r. Network Monitoring

s. Support for obtaining digital certificates and configuration of same with all related applications.

3.9.12. Wi-FI Solution at DC/DR, HO and RO

a. Management of the architecture –documentation of present architecture, peering management with ISP, access controls, user segmentation, policy and firewall management

b. Operation administration and Maintenance of the solution at all the locations.

c. Security and network management.

d. Routing on various devices at Ros

e. Coordination with all the relevant stakeholders.

f. End to end life cycle management.

3.10. IT Security Management

IT security management is a vast area involving logs at various devices including, firewalls and other security devices, password management, change management, etc. Hence, the required functionalities have been grouped under several categories as follows:

3.10.1. IT Compliance and Log Management

A suitable Syslog Server has to be incorporated with the following capabilities:

a. Collects logs from heterogeneous sources.

b. Decipher any log data regardless of source and log format

c. Rule-based event correlation for proactive threat management

d. Pinpoints breach attempts, insider threats, policy violations, and more, without any manual intervention

e. Generate pre-defined compliance reports for event logs and syslogs to meet various standard compliances like PCI DSS and etc.

f. Facilitate to create custom reports for new compliance to help comply with growing new regulatory acts demanding compliance in future.

g. Generate an alert in case of failure of log collection in regard with any log sources.

3.10.2. Incident Management Services

a. Perform continuous Monitoring on WAF and Web Proxy Consoles.
b. Prevention duties include system monitoring, assessment, testing, and analysis designed to identify and correct potential security breaches.
c. Protect and improve organizational security by preventing, averting, and mitigating security threats.
d. Perform following steps: Incident logging, Incident categorization, Incident prioritization., Incident assignment., Task creation and management., SLA management and escalation., Incident resolution.
e. Have collaboration with ITSM Security Team, ITSM Patch ITSM ITSM Service Provider and ITSM Network team to perform incident Analysis.
f. Analyze daily reports (AV reports network devices reports, IPS, etc.).
g. Creation and Maintaining of Tracker for incidents.
h. Perform RCA for Cyber security incidents (email phishing, Antivirus infections, repeated logout, etc.).
i. Preparing documentation for each incident analyzed.
j. Providing support for application-level settings at WAF.
k. Providing support for blocking /allowing any website at web proxy solution. Need to raise a ticket/case with OEM to resolve the website issue if any.
l. Miscellaneous Activities to be taken up by ITSM Service Provider

3.10.3. Firewall Security and Configuration Management

a. Centrally collect, analyze and archive logs from all security devices
b. Maintain firewall/UTM/SDWAN logbook for all devices location wise separately.
c. Automate compliance audits with reports for regulatory mandates such as PCI-DSS, ISO 27001, etc.
d. Perform firewall rule base review and device configuration analysis and Generate reports on quarterly basis.
e. Get real time alert on ‘who’ made ‘what’ changes, ‘when’ and ‘why’ to firewall configuration
f. Change management reports to get a complete trail of all the changes done to firewall configuration
g. Monitoring Internet usage (overuse and misuse) of employees
h. Monitoring outgoing traffic through the proxy, obtain details on user generating traffic, website access and bandwidth consumed
i. Real-time notification when a user tries to access restricted sites
j. Network traffic monitoring to get instant notifications upon sudden spike in bandwidth

k. Analysis of user or network activity consuming high bandwidth with interface-wise bandwidth usage reports

l. Getting detailed information on all possible network attacks and security breaches in organization's network

r. Knowing which viruses, malware, BOTs, APT, etc are active on the network, the hosts that are affected and more; Searching logs and report generation based on search results

s. Identifying highly used firewall rules which can be optimized to enhance network security

t. Identifying unused rules and/or modifying/removing them to improve firewall performance (to comply with all IS policy requirements of GoI/CISO)

u. All important GoI and Industry websites needs to be monitored regularly for various policy updates and with suitable approval from IT team of the Bank. All necessary and suitable policies should be applied by the ITSM Service Provider

v. Security Information and Event Management (SIEM)

w. The monitoring of endpoints, vulnerability information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS) and detection (IDS) systems

3.10.4. Privileged Password Management

a. Storage and organization of all privileged identities in a centralized vault

b. Secure sharing of administrative passwords with the members of the team on need basis

c. Self-resetting of passwords

d. Controlling access to IT resources based on roles and job responsibilities

e. Auditing of all privileged accesses and complete recording of all actions

3.10.5. Network Behaviour Anomaly Detection

a. Monitoring network security in real time

b. Monitoring internal and external threats

c. Classifying threats into various categories (e.g., DDoS, Scan/probe, Suspect, etc)

d. Carrying out detailed forensic investigation

e. Sending alert notification via Email or SMS

3.10.6. Active Directory Management and Reporting

a. Automatic routine AD management and reporting activities for AD administrators

b. Facilitates creation, management, and deletion of AD objects in bulk.

3.10.7. Self-Service Password Management

a. Allow users to reset/change their passwords and unlock their AD accounts, without IT intervention through web based portal using SMS and authenticator

b. Remind users automatically about soon-to-expire passwords by email and SMS

c. Allow users to update their profile details, like contact details in Active Directory through web based portal.

3.10.8. Network Configuration Management

a. Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI

b. Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes

c. Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.

d. Automating all repetitive, time-consuming configuration management tasks. Applying configuration changes in bulk to multiple devices.

e. Recording sessions: Getting complete record of who, what and when of configuration changes. Recording actions, archiving.

3.10.9. Active Directory Backup and Recovery

a. Automated incremental backup of Active Directory Objects

b. Change tracking to undo changes

c. Detailed version management to each attribute change

d. Provision to roll back Active Directory to an earlier state

3.10.10. Required ITSM Services

The ITSM Service team should be capable of performing the above stated activities using the prescribed tool(s). Some more key activities are:

a. Monitoring Status of security components and alerts, ports on firewalls

b. Monitoring Bounced Messages

c. Spam database update status

d. Monitoring Service Status (Up & Running),

e. Virus Alerts from Critical Servers

f. Logging security incidents

g. Assigning severity to the Incidents logged based on the definition.

h. First level analysis (investigating problems) and closure of known and low priority security incidents. Logging Problem Ticket for unresolved Incidents

i. Sending Security Alert messages on newly found vulnerabilities

j. Monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.

k. Maintenance of an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, solution servers, web servers, databases, security solutions, messaging solutions, etc.

l. Implementation of Change and Release Management

m. Installation of security patches & bug fixes

n. System health checks for all security devices

o. Vulnerability scanning

p. Adhering and Implementing guidelines and policies (BS7799)

q. Defining Rules in line with the security policy.

r. Responding to events and fixing vulnerabilities in IT infrastructure (like IPS, Checkpoint logs)

s. Implementation of Firewall exclusions

t. Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

u. Respond to security breaches or other security incidents and coordinate with respective OEM in case a new threat is observed to ensure that workaround / patch is made available for the same.

v. Maintenance and management of security devices including but not limited to maintaining Firewall services to restrict network protocols and traffic detecting intrusions or unauthorized access to networks, systems, services, applications, solutions or data protecting email gateways, Firewalls, servers from viruses.

w. Periodic reviews of domain level rights and privileges

x. Modifying access permissions and adding new access permissions of security policies on existing firewall.

y. Up-gradation of the firewall and IPS devices.

z. Signature update for IPS device.

aa. Configuration backups for all security devices

bb. Syslog server configuration & management including review of logs.

cc. Managing / monitoring the IDS/IPS tool and policies as per guidelines of NABARD.

dd. Modifying the policy for IDS/IPS/Firewall based on observed trends / security lapses.

ee. Changing network address translation rules of existing security policies on the firewall.

ff. Adding new network address translation rules on security policies on existing firewall.

gg. Diagnosis and troubleshooting of the problem faced on firewall and faced by the IDS/IPS.

hh. Managing / monitoring the IDS/IPS tool and policies

ii. Periodic / Critical reporting to NABARD officials based on Firewall / IDS / IPS activities

jj. Managing configuration and security of Demilitarized Zone (DMZ)

kk. Alert / advise NABARD about any possible attack / hacking of services, unauthorized access / attempt by Mental or external persons etc.

ll. Resolution and restoration of services in case of any possible attack and necessary disaster management

mm. Shutdown of critical services to prevent attack (internal or external)

nn. Advise to improving network/Data Center security to protect NABARD's data / information from both internal and external persons/attack.

oo. Resolution and restoration of services in case of any possible attack and necessary disaster management.

pp. Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.

qq. And other related essential activities to ensure that the functionalities of IT Security.

3.10.11. Checkpoint/Fortinet/Forcepoint/SDWAN Security Requirements

The Security Engineer should be skilled to carry out the following areas and should be a Certified Security Administrator.

a. Install the security gateway in a distributed environment

b. Configure rules on Web and gateway servers

c. Create a basic rule base in Smart Dashboard and assign permissions

d. Schedule backups and seamless upgrades with minimal downtime

e. Monitor and troubleshoot IPS and common network traffic

3.10.12. The Security ITSM Engineer should be capable of the following:

a. Be prepared to defend against network threats

b. Evaluate existing security policies and optimize the rule base

c. Manage user access to corporate LANs

d. Monitor suspicious network activities and analyze attacks

e. Troubleshoot network connections

f. Protect email and messaging content

3.11. Data Base Administration

3.11.1. Database monitoring

- **a.** Creating user-specific SQL or PL/SQL metrics with warning notification
- **b.** Execution of user-specific scripts on Windows platform
- **c.** Creating customized SQL reports with email notification
- **d.** Dynamic visual indication of problems in the console

3.11.2. Instance access to the following information

- **a.** Size of databases
- **b.** Free space in table spaces
- **c.** User table spaces, spaces occupied by objects
- **d.** Object/system privileges of users/roles, reasons of granting
- **e.** List of roles/privileges granted according to a certain document
- **f.** Description of users, their passwords, reasons for creation
- **g.** List of scripts in a specific database and their purpose
- **h.** Technical documentation of any database
- **i.** Log of actions/crashes/incidents in any database
- **j.** And other related areas.

3.11.3. Log of database changes

- **a.** Date of creation/deletion of users/roles, log of privilege changes
- **b.** Time of granting/revoking privileges, reasons for granting
- **c.** Table space sizes
- **d.** Time and date of database objects creation and deletion
- **e.** History of database operations performed in the system (e.g., granting of privileges, creation of table spaces, etc.)
- **f.** Connections to the database, with names of computers and solutions
- **g.** And other related areas.

3.11.4. Automation of routine operations

- **a.** Moving of tables. Automatic detection of available table spaces for moving
- **b.** Automatic rebuilding of indexes invalidated during the moving of tables of their partitions
- **c.** Quick creation of table spaces, automatic naming
- **d.** Adding and resizing files, automatic naming
- **e.** (v) Splitting, exchange and removal of table partitions. Support of partitioning by various criteria (dates, interval).
- **f.** and revocation of system or object privileges using lists
- **g.** User creation and editing
- **h.** Top queries by CPU
- **i.** Top Queries by IO
- **j.** Top CLR Queries and Waits
- **k.** Top Slow Running Queries

l. Frequently Executed Queries
m. Most Blocked Queries
n. And other related areas.

3.11.5. Storage of documents and descriptions

a. Storage of database descriptions, their versions, paths, etc.
b. Descriptions of users and their passwords stored in an encrypted form
c. Comments to the privilege being granted (including the preferred revoking date to be monitored)
d. Comments to database files, table spaces, warnings
e. Action, crash or incident logs for each database
f. Descriptions of SQL and OS scripts, their relation to bases and hosts
g. Technical and work documentation on any database
h. And many more.

3.11.6. Required Services

The Data Base Administration (DBA) should be familiar with following DBA activities. Some more important activities include:

m. The DBA services shall cover existing production, testing & development DB environments that are in the organization at all locations.
n. New DB implementation , migration support and services& Services for Microsoft SQL 2012, 2016, 2019 , Oracle 11g , 12c, 19c, Mysql 7,8 , Postgres, PGsql & higher versions. Support and operation for any forthcoming application databases other than listed above.
o. –Specific activities only need to be handled by ITSM team. Enterprise application owners will be taking care of applications. Primary ownership will be with application owners and primary work to be done by enterprise application owners.
p. Change management of database schema, storage, disk space, table space, user roles, backup and purging etc.
q. As per IT security policy of the organization, ensure database patch management with minimum downtime and recommend appropriate patches of Operating System relevant to database.
r. Managing database upgrades operations. Including minor and major upgrades of all existing and newly introduced applications in future.
s. And other similar activities.
t. Advisory services to enhance application performance and user experience, user role management.
u. Proactive cleaning of extra tables.
v. Provide automation support.
w. Integration with different platform and systems.
x. Audit activity to be done frequently to review database schema, storage, disk space, table space, user roles, backup and purging etc.

3.12. Vendor Management

ITSM Service Provider should be familiar with installation, configuration and usage of the prescribed vendor management tool and should carry out the following responsibilities:

3.14.8. Coordinate with vendors for support services.

3.14.9. Logging calls, tickets, coordination and follow-up with vendors

3.14.10. Escalation of calls to the higher levels at vendor side in case of requirement.

3.14.11. Vendor SLA tracking and monitoring with alerts and escalations (including WAN Vendor)

3.14.12. AMC/ Warranty/ Support Tracking

3.14.13. Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the vendor will be made separately by NABARD)

3.14.14. Management of assets sent for repair.

3.14.15. Maintain database of the various vendors with details like contact person. Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with vendor Coordinate and follow up with the vendor and ensure that necessary spares exchanged.

3.14.16. Analyze the performance of the vendor periodically (Quarterly basis or as specified).

3.14.17. When a new solution (Hardware/software) is introduced, training to engineer/users to absorb and leverages the technology for business should be invariably arranged. And other related activities.

3.14.18. End to end lifecycle management of new solution (Hardware/software).

3.13. Help/Service Desk Services Management

The related ITSM Service Provider should be capable of installation, configuration and using the above said help/service desk tool and carry out the following activities:

3.13.1. Helpdesk resource should log all ticket received through various channels e.g. phone, email, IVR, sms, chatbot, MS-teams etc.

3.13.2. The Help desk team should be able to post the response back to the concerned people.

3.13.3. Helpdesk should classify and assign the ticket in appropriate section of ITSM services and other NABARD internal applications

3.13.4. Helpdesk tool should include tickets of all ITSM as well as NABARD internal applications and assign them to respective application teams.

3.13.5. If needed, the concerns/service requests can be escalated to concerned IT team who will be able to look into it.

3.13.6. Generate status report of pending/closed concerns on a daily/weekly/monthly basis.

3.13.7. Helpdesk should ensure that all calls to IT helpdesk are logged at a central helpdesk. All calls logged will have to be monitored and assigned to respective team /engineer / analysts and tracked for proper closure within the specified SLA limits. Helpdesk would ensure that the calls should be updated with the diagnosis carried out to close the call.

3.13.8. The service provider shall ensure that any change in resident engineers and/or helpdesk personnel is conveyed to the concerned NABARD officials one month in advance. The ITSM Service Provider would provide resumes of proposed ITSM resources (engineers/helpdesk personal)to the concerned NABARD officials. Only approved resources would be permitted to replace the outgoing ones.

3.13.9. The helpdesk shall provide support for distribution of computer peripherals on demand and maintain inventory of the same.

3.13.10. And should carry out other similar activities.

3.14. Non-Delivery of Services / PENALTIES & SLAs

3.14.1. The selected ITSM Service Provider will have to provide satisfactory service to achieve the service levels as given in "Expected Service Delivery". The service level performance will be recorded/monitored daily and will be reviewed on quarterly basis and non-performance will result in penalty being imposed.

3.14.2. The tools provided for monitoring and managing these services should give a detailed report for calculating the support calls including the response time, resolution time, penalty cost applicable etc. This should facilitate both the Service Provider and the Bank to directly arrive at the penalty cost applicable under all these services.

3.14.3. The total non-performance charges for a quarter will be calculated and deducted from the quarterly bill of the selected ITSM Service Provider. Annual Contract value will be calculated on the basis of the opening quarterly inventory after adjusting the addition or deletion, if any, during the previous quarter.

3.14.4. Penalty charges would be applied for those services, which have not achieved the stipulated service levels based on the table mentioned in Expected Service Delivery. There will be maximum penalty charge of 10% per Quarter of the Quarterly Contract value.

3.14.5. The calculation of the same will be done on a Quarterly basis as under - At the end of every month, the ITSM Service Provider will submit the average response time and average resolution time report. Rs 500/- per hour subject to a maximum of Rs. 3000/ per day for critical equipment and Rs. 300/- per hour subject to a maximum of Rs. 1500/- per day for all other equipment. Within 5 working days the original equipment should be delivered back to us.

3.14.6. Table for all ITSM services rating will be formulated in discussion with NABARD.

3.14.7. Spare Parts

3.14.7.1. If the original asset is not returned in the stipulated 5 days, a penalty of Rs. 2000/- per day for critical equipment and Rs. 1000/- per day for other equipment would be levied.

3.14.7.1. In case of a genuine problem of non-availability of spare parts with the principal, a letter / email to that effect should be forwarded to NABARD by the ITSM Service Provider. NABARD at its discretion may decide to waive off the penalty in such exceptional situations.

3.14.8. Covering for Absence of ITSM Services

3.14.8.1. The backup engineer in the centers should be trained in the presence of the main engineer and if need be, the backup engineer could be asked to manage the infrastructure in the supervision of the main engineer, for a couple of days. This will lead to a seamless backup of the main engineer when he avails of short spells of leave. Service provider should ensure that same engineer is available in absence of main engineer

3.14.8.2. In case suitable replacement is not given for leave/resignation/reassignment of ITSM personnel, a penalty of Rs.1000/- per day per personnel towards absence will be imposed. In case the resident officials are absent / late and a suitable replacement is not provided, a penalty of Rs. 200/- per hour subject to a maximum of Rs 1000/- per day will be imposed.

3.14.9. Expected Service Delivery

Sr No	Particulars	Response	Resolution	Penalty
1.	Desktops of Critical (such as Dealers at H.O, Risk Team) Depts. And Senior Officials at H.O.	15 minutes	30 minutes or immediate standby to be provided	Rs. 500/- per working hour delay or Rs. 3000/- per day whichever is less.
2.	Other Equipment: Desktops, Applications,	30 minutes	2 hours. (1 working day if parts are to be replaced)	Rs 300/- per working hour delay or Rs

	Printers, Scanners, etc. at H.O.			1500/- per day whichever is less.
3.	Laptops	30 min.	2 working days if parts are to be replaced.	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
4.	Resolution of OS related problems	30 min	12 hours	Rs. 500 per working hour delay or Rs 3000/- per day whichever is less.
5.	Servers, Network and related equipment, and all other equipment under warranty	30 min	Follow up, Co-ordination & Escalation within 4 hours	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
6.	R.O. Desktops, Laptops - OS / Application issues	30 minutes	2 Hours	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
7.	R. O. Desktops, Laptops - hardware issues	30 min	2 hours for troubleshooting and logging call with OEM for replacement of part / warranty machine.	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
8.	R. O. MPLS related issue	30 min	2 hours for troubleshooting and resolution / providing report on findings.	Rs 300 per working hour delay or Rs 1500/- per day whichever is less.
9.	Issues with Tools provided by the ITSM Service Provider	30 min	Follow up, Co-ordination & Escalation within 4 hours	Rs 500 per working hour delay or Rs 3000/- per day whichever is less.

3.14.7.1. The response & resolution time will be calculated from the time of lodging the call. When formatting and loading of all the software is required, additional two hours will be allowed for resolution. For calculating downtime, calls logged after closing time will be treated as logged at the opening hour of the following working day. Resolution time includes making the systems available for work with O/S uploaded.

3.14.7.1. ITSM Service Provider has to make alternate arrangements for leave/resignation/reassignment of ITSM personnel and intimate the same to NABARD at least one month in advance. A penalty of Rs. 1000/- per day per personnel towards absence will be imposed, if suitable replacement is not given (with the qualification & experience)

3.14.7.1. Also, to service the most obsolete or discontinued model as well, the ITSM Service Provider shall be liable for any loss or damage to the scheduled equipment caused due to negligence of the ITSM Service Provider during the contract period.

3.14.10. DOWNTIME - CALCULATION METHODOLOGY

3.14.10.1. 'UPTIME' of the hardware and system software = (Reckoned Hours minus Downtime /Reckoned Hours X 100 for the maintenance year.

3.14.10.2. Reckoned Hours = Uptime commitment per day X No. of committed days per Year

3.14.10.3. Uptime Commitment per day = Hardware and System Software Maintenance Support Time per day

3.14.10.4. Down Time will be counted from the time of reporting the maintenance call by NABARD to the ITSM Service Provider till the resolution of the problem / operations of the hardware and system software.

3.14.10.5. No. of committed days per Year = the number of working days of the NABARD during the year.

3.14.11. NON-PERFORMANCE CHARGES:

3.14.11.1. The selected ITSM Service Provider will have to provide satisfactory service to achieve the service Levels as given in Expected Service Delivery table. The service level performance will be recorded/monitored daily and will be reviewed on quarterly basis and non-performance will result in penalty being imposed.

3.14.11.2. The total non-performance charges for a quarter will be calculated and deducted from the quarterly bill of the selected ITSM Service Provider. Annual Contract value will be calculated on the basis of the opening quarterly inventory after adjusting the addition or deletion, if any, during the previous quarter.

3.14.11.3. Penalty charges would be applied for those services, which have not achieved the stipulated service levels based on the table "Expected Service Delivery" as mentioned above. There will be maximum penalty charge of 10% per Quarter of the Quarterly Contract value.

3.14.11.4. At the end of every month, the ITSM Service Provider will submit the average response time and average resolution time report.

3.14.11.5. The calculation of the same will be done on a Quarterly basis as under:

Rs 500/- per hour subject to a maximum of Rs. 3000/ per day for critical equipment) and Rs. 300/- per hour subject to a maximum of Rs. 1500/- per day for all other equipment. Within 5 working days of the original equipment should be delivered back to us.

3.14.11.6. The ITSM Service Provider may keep all IT assets in buffer stock in ready to use condition. The ITSM Service Provider may provide machine from buffer stock within 30 minutes from user request. If the machine is not provided in stipulate time, a penalty of Rs. 300/- per hour and Rs. 1500/- per day would be levied.

3.14.11.7. In case of a genuine problem of non-availability of spare parts with the principal, a letter / email to that effect should be forwarded to NABARD by the Principal. NABARD at its discretion may decide to waive off the penalty in such exceptional situations.

3.14.11.8. Non-performance charges will not be applied for that equipment under ITSM Service Provider management provided the calls are logged within the response time to the respective ITSM Service Providers and followed up with proper escalation.

3.14.11.9. In case suitable replacement is not given for leave/resignation/reassignment of ITSM personnel, a penalty of Rs.1000.00 per day per personnel towards absence will be imposed.

3.14.11.10. In case the resident officials are absent / late and a suitable replacement is not provided, a penalty of Rs. 200/- per hour subject to a maximum of Rs 1000/- per day will be imposed.

3.14.11.11. ITSM service provider will incorporate all above mentioned rules and conditions in their tool and provide online access to DIT management. They will also provide monthly and quarterly penalty sheet.

3.15. Advisory Services

NABARD also will like to have advisory services by competent personnel of the ITSM Service Provider as part of ITSM Services. The ITSM Service Provider shall arrange for presenting a summary of the IT Services provided to the Bank vis a vis the best practices in the industry and shall make efforts to ensure that they are assimilated in the Bank.

Service Components	Documents/Reports to be shared by ITSM personnel with NABARD (along with Frequency)
Storage Management	(i) Effective storage management (ii) Capacity planning (iii) Suggesting best practices about back up
Data Center and Server Management	(i) Best industry practices (ii) Capacity planning
Network Management	(i) Advisories for revamping networks (ii) Periodic review for service improvement (iii) Best Industry Practices
IT Security Management	(i) Advisory for firewall/IDS/IPS rules (ii) Potential/emerging threats and preventive measures (iii) Best Industry Practices

3.16. Resource

Staffing/ Skill-Set / Qualification / Experience /Knowledge Sharing

3.16.1. HO onsite engineers - as per Bank's understanding a total of 25 engineers with necessary skillsets as indicated the Appendix III. However, the ITSM Service Provider is expected to propose a suitable team structure, composition and number of engineers after doing a complete study of the RFP document.

3.16.2. At all other 35 ROs & TEs locations, full time onsite engineers has to be placed as per details mentioned in Appendix III. He/she will be responsible for delivery, Management of all above said service components.

3.16.3. The key parameters for evaluating the team members would be:

- **e.** Qualification & Certification
- **f.** Total experience
- **g.** Number of similar analytics assignments handled
- **h.** Number of similar project duration assignments handled

The number of service engineers indicated in the table below is prescriptive only. The total number engineers needed for providing all the services sought at various locations (on-site and off-site) should be worked out so as to maintain the SLA standards and accordingly the solution should be built and provided.

The detailed break-up of project team members, their summarized job description and evaluation criteria are tabled below:

Sr. No.	Staff Profile	Job Description	Skill - set / Qualification / Experience /Knowledge sharing /Qualification & experience
1	Team Lead	Responsible for overall performance and delivery of the ITSM Services.	MCA /B. Tech / BE
		Should be Pro-Active	Mandatory certification: ITIL certified
		Should efficiently document and share with team and NABARD	Minimum 8 years of relevant experience as a IT Team Leader
		The team lead would be Accountable: Being held accountable for the RFP implementation and shall ensure seamless services.	Demonstrated service delivery experience & application support experience, preferably in a 24x7 environment

		Ensure Fair and Timely Reporting	Experience in the use of an issue Logging, assigning and tracking system (Ticketing System)
			Effective computer skills; Microsoft Office
			Effective communication skills both verbally and in writing.
			Experience of ITIL practices
			Coordination with all technical teams for troubleshooting and RCA
2	IT Help Desk Executive	Incident Management - Logging of calls from Users, departments and other engineers, raise tickets assign it to engineers	Minimum 3 years of relevant experience
		Follow-up for call closure and escalate wherever necessary. RFO to be ensured.	Experience in IT helpdesk services
		Share incident/problem report on daily, weekly and monthly basis.	Basic understanding of computer technology in a business environment. Effective computer skills; Microsoft Office
			MS outlook Email client, Helpdesk / Ticketing software applications.
			Effective communication skills
			Knowledge of ITIL processes
3	System Administrator Windows, Linux, AIX	Installation, configuration, monitoring, fine tuning, troubleshooting of servers and VDI Infrastructure	1. Relevant Experience - 5 years
		Prepare & share availability reports with NABARD core IT team	2.Degree/Diploma in Computer Engineering, MCSE Certified, CCNA, RHCE, IBM AIX Administrator

		VM creation and Management	3. Experience in Windows Server 2008, 2012, 2016, 2019 and upcoming Versions Windows 10, 11 and upcoming Versions RHEL, CentOS, Ubuntu, Debian 7, 8, 9 and upcoming Versions. AIX v7 and above.
		Physical server setup and troubleshooting. He Should be well versed with DHCP, DNS, WINS, WSUS SMTP, PO3 RAS VPN SAN, Cluster environment, Back up etc.	4. Wide range trouble shooting skills involving, OS, Active Directory, LDAP, storage, security, DNS/ DHCP, DFS, printers, network, database, webserver management apache, tomcat, Jboss, IIS, Nginx, weblogic, websphere etc.
		Patch management OS, DB, servers, desktops, devices, BIOS, switches, firewalls, IOS, firmwares	5. Experience in Hyper-V, ESXi, Nutanix AHV, KVM hypervisors
		Enterprise Antivirus Updates and Patches.	6. Experience with tower, Blade and Rack mounted workstations,
		Email ID Creation & backup	7. Experience with thin clients (setup, configuration, and management)
		Complete backup of Data and Device configurations	8. Experience managing, monitoring, scaling, and implementing large enterprise level virtual desktop and application virtualization environments.
		Identification and resolution of individual and system issues which result in or potentially result in disruption to services provided	9. Experience with disaster recovery of Microsoft Active Directory and Windows and Unix Servers
		Participate in internal and external projects, reactive and proactive maintenance,	10. Knowledge of storage technologies (NFS and iSCSI SAN, NAS)

		sustaining, RCA and break-fix activities	
			11. Linux (Suse, Red Hatt) Support
			12. Cisco/Virtualisation (Server & Desktop)
			13. Knowledge of storage technologies (NFS and iSCSI SAN, NAS), Linux (Suse, Red Hat, Ubuntu, AIX) support and Cisco/Brocade, Virtualisation (Server & Desktop)
4	DBA Personnel - Oracle, MySQL	The role will be Database Administration, installation, replication, clustering, Troubleshooting and performance tuning of databases components, taking regular backups on windows, linux and AIX.	BE/BTech/MCA
		Duties include but are not limited to Maintenance/ administration of the database	Total experience: Minimum 5 years of post-qualification experience in Database management in Oracle DB 11g ,12c, 19c and higher. MySQL 7,8 and latest Relevant Database administration certified. Oracle certified DBA (OCP)
		Space management/user management	Relevant Database administration certified
5	DBA Personnel - MS SQL	1. The role will be Database Administration, Troubleshooting and performance tuning of databases components, taking regular backups	BE/BTech/MCA
		2. Duties include but are not limited to	Total Experience: Minimum 5 years of post-

		Installation, replication, clustering, Maintenance/ administration of the databases	qualification experience in Database management in MS SQL Server 2012,2014, 2016, 2019 and higher.
		3. Space management/user management	Relevant Database administration certified. Microsoft Certified DBA (MCDBA)
6	Nutanix Administrator	Installation maintenance and management of Nutanix clusters	Nutanix certified professional (NCP MCI 5)
			Should have hands-on experience of 4 Years on Nutanix cluster installation, monitoring, maintenance and management
			VM Replication, Flow, LEAP, Xplay, disaster recovery.
7	Security Support	Refer Scope of Work.	1. BTech, B.E. / Graduate with relevant Experience - 2 years Fortinet Certified Network Security Administrator (FCNSA)
			2. Certified Forcepoint NGFW Administrator
			3. Check Point Certified Security Administrator (CCSA)
			2. Hands on experience in Maintaining a PSS environment.
			3. Hands-on experience on Firewall devices, VLAN, Proxy
			4. Reporting skills & good interpretation skills
			5. Excellent communication skills
			6. Knowledge on Network Security protocols
8	Network Engineer	Refer to Scope of work.	1. B Tech / Graduate in Computer Engg, E&C or Computer Application. , CCNA is compulsory.

			Juniper Networks Certification Program (JNCP), JNCIA-JunOS
			2. Total 2 years should be working as Network Engineer. Hands-On experience on big multisite LAN and WAN network.
			3. Should be able to solve all the monitoring part mentioned under Scope of work and should be able to act as first point of support for all DC/DR/HO/RO calls.
9	Backup Executive	Configure new backup, Monitor and manage backup operations. Restore data on requirement.	B Tech, B.E. / in Computer Engr E&C or equivalent. Hands-on experience on high-end storage and tapes. Hands-on experience on HPDP and Arcserve backup. Minimum of 3 years' experience is required in the relevant area.
10	Regional / Corporate Office Service Support Engineer	Desktop/Laptop on-site and phone support	1.Travelling to branches / ITSM Service Provider sites within the region would be involved with this position
		Printer/Scanner support	2.Minimum 1 years of relevant experience
		Backup system support- Updating current infrastructure	3.Desktop and Network Troubleshooting
			4.Installing and configuring Operating Systems (Windows7, 8.1, 10, 11, Linux) Installing and configuring Application Software (MS Office, Open Office, .net and Java, email clients, all client software, etc.)
		VC support	Engineers should be able to manage/operate legacy VC services/MS Teams/Webex etc. from Mumbai location to

			various regional offices/ training establishments of NABARD
		Deploying new equipment	5.Installation and configuration of all applications Configuration of printers, scanners, projectors
		Provide investigation, diagnosis, resolution and recovery for hardware /software problems	Graduation, Diploma in any discipline. Certifications: CompTIA Network+, Network 5 Certification, Microsoft Certified Desktop Support Technician (MCDST) Microsoft Certified System Administrator windows 10 (MCSA) Two Years hands-on experience in installation and troubleshooting of windows operating system, application software's, peripheral devices and networking devices. Hands-on experience of basic networking. Working knowledge of ticketing system, ticket resolution and follow-up Working knowledge of online meeting setup and video conferencing. Good verbal and written communication.
		Maintain overall ownership of user's issue & service ensuring that they receive resolution within a stipulated timeframe	
		Manage service requests, software installations, new computer setups, upgrades, etc.	

		Record incident resolutions in the Help Desk tool.	
		Provide enhancement request feedback to IT regarding technology environment and customer needs through the defined processes.	
		Support the following technologies: Windows 10,11 Microsoft Office 365 products - Outlook, Word, Excel, Access, Internet Explorer, etc. desktops, laptops, printers, networked copiers, basic LAN/WAN connectivity and others as assigned.	
		Monitor daily backups.	
		Please refer scope of work	
		All relevant components in SoW	
11		Installation and troubleshooting of windows 7, 8, 10, 11 etc Install application softwares, updates, upgrades of endpoints. Monitor daily backups. Installation and troubleshooting of printers, copiers, scanners, plotters, projectors, webcams, switches, firewall, UTM, video conferencing devices etc.	

		Install new devices, log tickets for AMC support. Resolve day to day user and network issues and improve user experience. Provide onsite support to senior officials	

Note: The qualifications and skill sets outlined above are minimum expectations only. Depending on the roles and responsibilities needed under a service domain, the engineer/s should have additional qualifications/skill -sets. All certifications should be active for next 2-5 years.

3.17. General

3.17.1. Service period: NABARD intends to avail these services for a period of 5years and extendable by 1 year.

3.17.2. Knowledge Transfer and Handshake between existing and new ITSM Service Provider will be of maximum 2 months from date of PO.

3.17.3. ITSM Service Provider will be responsible for all changes as per "Change Management Process" (Given in Annexure).

3.17.4. All resources will be appointed after screening / interview by NABARD.

3.17.5. NABARD has right to change any resources deputed by ITSM Service Provider, replacement of any such resource should be completed in 30 days from the date of intimation by NABARD.

3.17.6. NABARD will conduct quarterly review performance of all resources deployed by ITSM Service Provider. If performance of any resource is not satisfactory, ITSM Service Provider will replace of any such resource within 30 days from the date of intimation by NABARD.

3.17.7. All changes in ITSM resources should be informed to NABARD one month in advance and NABARD will be part of all handover activities.

3.17.8. The ITSM Service Provider shall provide complete services as per the scope including mounting, unmounting, installation, implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.

3.17.9. The ITSM Service Provider shall ensure that during various phases of implementation, the performance, security, network availability, etc. of the existing network setup should not be compromised.

3.17.10. ITSM Service Provider shall provide a well-maintained Documents to NABARD

3.17.11. The ITSM Service Provider shall support for replacement and upgradation of out-of-support, out-of-service, end-of-life (EOL), end of support (EOS) undersized infrastructure elements as soon as the respective OEM announced the same at no additional cost to the bank throughout contract period. The ITSM Service Provider shall inform NABARD within 15 days of announcement.

3.17.12. The list mentioned above is the indicative list; however, the successful ITSM Service Provider should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the Bank.

3.17.13. The ITSM Service Provider shall adhere to the Service Level Agreements (SLA) and regular monitoring and reporting it to the bank.

3.17.14. The ITSM services should be compliant with Bank's IT, IS, e-mail and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.

3.17.15. The ITSM processes should comply with RBI cyber security circular no. RBI/2015-16/418 dated 2 June 2016 and its annexure 1- Baseline controls(including all relevant circular and update to same by RBI).

3.17.16. The ITSM process should be of ITIL 4.0 processes for Bank requirements related to change, incident, problem, configuration management, SLA and capacity management etc.

3.17.17. The ITSM Service Provider should follow a standard process to ensure that proposed solution meets functional, security performance and regulatory requirements of the bank. The selected ITSM Service Provider shall be responsible for proactive health monitoring of infrastructure on 24x7x365 basis.

3.17.18. The Bank has a complex infrastructure with multiple resources maintained and managed through multiple ITSM Service Providers. The ITSM Service Provider shall coordinate with all other ITSM Service Providers for seamless integration, implementation and operations

3.17.19. The ITSM Service Provider shall prepare the SOPs (Standard Operating Procedures) with periodical review as per industry practices and regulatory guidelines. The drafted SOPs shall be submitted to the Bank for its review and Approval.

3.17.20. The ITSM Service Provider shall configure the SLA Levels for all applications (including hardware & software) in IT Service Management tool with the functionality of auto-escalation of incident/ticket to appropriate bank authorities in case of breach of defined timelines for resolution of incident/ticket.

3.17.21. The ITSM Service Provider shall integrate all Bank assets (Servers, Storage, Network devices) in the monitoring tools and provide the unified Dashboard for monitoring & Management of devices.

3.17.22. The ITSM Service Provider shall be responsible for patching of Bank managed servers, all desktops connected in Bank network as per frequency of patches released by product OEM.

3.17.23. The ITSM Service Provider shall ensure patching & hardening for all Bank managed servers, and get the same cleared from the Information Security Cell /SOC of the Bank. The ITSM team has to prepare a patching calendar as per the frequency of the patch released by the OEM team and share the same with the bank team. The patches have to be applied in the same month in which OEM has released the patches as per prescribed as defined in SLA.

3.17.24. The ITSM Service Provider should retain all logs including DHCP and security logs for a period of 02 years, quarterly backup of all logs including logs from tools should be provided to NABARD.

3.17.25. For any incident, Service Request, VAPT/Audit/NAC – The project manager may co-ordinate with all stakeholders in order to follow up for closure of all observations.

3.17.26. Patching support for all components of all installed & authorised software, OS patches, antivirus patches and BIOS updates.

3.17.27. Special Note:

3.17.27.1. 24 x 7 Support requirement with combination of onsite & offsite support. Onsite support is required for General shift(9AM to 6 PM) during normal working days. Support for remaining period is required on a call or remote basis. In case the issue cannot be resolved remotely, the SME (Subject matter expert) is expected to travel to our site for support.

3.17.27.2. VAPT support and compliance management (Review, General)

3.17.27.3. If required, for all scheduled and troubleshooting activities onsite engineers should be available on Saturdays/Sunday/Holidays

3.18. Miscellaneous services

ITSM Service Provider will provide following miscellaneous services:

3.18.1. In the event of shifting of office premises / Data Centers / Disaster Recovery Centers / Near Disaster Recovery Centre by the Bank, ITSM Service Provider would depute Facility Managers / engineer(s) for de-installation of all the hardware, coordinate with 3rd party vendors, supervise packing/transportation and installation/ commission of equipment at new location. No extra cost will be borne by the Bank for the same. However, packing and transportation will be arranged by the Bank separately.

3.18.2. In the event of adding new office at new locations by the Bank, ITSM Service Provider has to assist the Bank in setting up of LAN (cabling, I/O fixing etc.) coordinate with network vendor for setting up of WAN connectivity etc. Cost towards raw material will be borne by the NABARD. As & when the Bank opens its new office it is the responsibility of the ITSM Service Provider to provide ITSM engineer on call basis as per the contracted rate.

3.18.3. Suggestions/ Recommendation to improve the current infrastructure architecture for better response & security.

3.18.4. ITSM Service Provider shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed in the Bank. The Bank will provide the list of all the authorized software and the number of licenses procured.

3.18.5. If Bank implements any project in future, then the ITSM Service Provider shall provide required support.

Schedule B

Documentation

1. ITSM Service Provider will provide support for coordinating with other external vendors (such as ISPs etc. providing IT services to NABARD) for resolution of the problems related to IT issues/projects. The Scope covers the IT vendors of NABARD at all locations.

2. Documentation & Reporting Deliverables:

- **a.** Maintaining database of the all vendors
- **b.** Contact person/Telephone / Fax / Email, etc
- **c.** Escalation Matrix / Response time
- **d.** Co-ordinate with vendors for email technical support & other technical problems.
- **e.** Generate reports of calls logged, resolved, escalated and pending with time and date and monitor vendor performance using tools.
- **f.** NABARD software/hardware configuration, network diagrams documentation.

3. Technical Documentation

3.1. Following documents should be delivered by the ITSM Service Provider to the Bank for every software including third party software before software/service become operational, which includes, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures etc.

3.2. The ITSM Service Provider should also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable. The ITSM Service Provider should also provide the MIS reports as per requirement of the Bank. Any level/version changes and/or clarification or corrections or modifications in the above-mentioned documentation should be supplied by the ITSM Service Provider to the Bank free of cost in timely manner.

4. Reports

ITSM Service Provider shall submit the reports on a regular basis in a mutually decided format. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients. ITSM

Service Provider shall submit certain information as part of periodic review as and when required by the Bank

Following is the indicative list of reports:

4.1. Daily reports (to be submitted on next working day)

- **a.** Log of backup and restoration undertaken.
- **b.** Summary of issues / complaints logged at the Help Desk.
- **c.** Summary of resolved, unresolved and escalated issues/complaints.
- **d.** Summary of resolved, unresolved and escalated issues/complaints to OEMs/SP/NABARD support teams.
- **e.** Mail traffic report - list of top users sending /receiving highest number of mails.

4.2. Weekly Reports (to be submitted on the first working day of the following week)

- **a.** Issues/Complaints Analysis report for virus calls, call trend, call history etc. Summary of systems rebooted.
- **b.** Summary of issues /complaints logged with the OEMs.
- **c.** Summary of changes undertaken in the Data Center including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset etc.

4.3. Monthly Reports (to be submitted by 10th of the following month)

- **a.** Component wise physical as well as IT infrastructure availability and resource utilization.
- **b.** Summary of component wise Data Center uptime.
- **c.** Summary of changes in the Data Center.
- **d.** Log of preventive / scheduled maintenance undertaken. Configuration Management summary report.
- **e.** Change Management summary report.
- **f.** Release Management summary report.
- **g.** Service Level Management - priority/severity wise response and resolution.
- **h.** Service Failure Analysis, listing out escalations and downtime/outages, if any.

4.4. Account Dash Board, listing out:

- **a.** Planned activities carried out during the month.
- **b.** Unplanned activities carried out during the month.
- **c.** Activities planned but missed specifying the reasons.
- **d.** Challenges faced during the month.

4.5. Service Operations, listing out:

a. Service Desk Management - Location wise call summary for all on-site ITSM locations for last three months.

b. Helpdesk Management, listing out priority/severity wise calls logged with comparison for past three months.

c. Incident Management, giving category wise call details for critical overhaul areas with comparison for past three months.

4.6. Operational Activities

a. Location wise weekly visits done for off-site ITSM and attendance of the on - site resource personnel.

b. Service wise performance of activities as per scope of individual service areas.

4.7. Service Improvement Plan, listing out:

a. Concerns/Escalations with action plan.

b. Planned activities/initiatives.

c. Improvements planned, if any.

4.8. Incident reporting (to be submitted within 48 hours of the incident)

a. Detection of security vulnerability with the available solutions / workarounds for fixing.

b. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. - with root cause analysis and the plan to fix the problems

c. Software license violations.

4.9. The ITSM personnel are required to provide various documents/reports to NABARD on a time-to-time basis. Few important of them are highlighted here. the detailed Scope of Work may mention about many other such requirements.

S. N o.	Service Components	Documents/Reports to be shared by ITSM personnel with NABARD (along with Frequency)
1.	AMC for Computers and Peripherals	Onsite maintenance service reports (daily)
2.	Inventory Management	i. List of hardware's (always updated - to be shared whenever required) v. List of software's (always updated - to be shared whenever required) vi. List of licenses along with expiry dates, how many deployed, etc. (always updated - to be shared whenever required) vii. Configuration change report (whenever configuration changes)

3.	Patch Management	iii. List of installed and missing patches (always updated - to be shared whenever required) iv. List of devices where patches have been applied but not yet activated (always updated - to be shared whenever required)
4.	Domain Services Management	iv. List of all users, associated computers, and access permissions (always updated - to be shared whenever required) v. Change requests (whenever it arises) vi. Audit report of administrative privileges (weekly)
5.	Storage Management	v. Storage server availability report (daily) vi. Network reachability report (daily) vii. Log of backups taken (weekly) viii. Capacity Planning Report (monthly)
6.	Data Center and Server Management	vii. State of environment and power conditions (daily) viii. Assessment of data center in terms of cooling, power, positioning of racks, and other health parameters (first report after 2 months, and subsequently once in a year) ix. On-site inventory of critical equipment for the data center (always updated - to be shared whenever required) x. Log register of visitors in data center (daily) xi. Server availability report (daily) xii. Audit of server logs (weekly)

7.	Network Management	ix. Inventory of network hardware (always updated - to be shared whenever required) x. Logs of switches/routers (weekly) xi. Status of the switches/routers (daily) xii. Status of the links (daily) xiii. Traffic patterns (weekly) xiv. Analysis of which user is consuming more bandwidth within the network (daily) xv. Report of network configuration changes (whenever such change occurs) xvi. Periodic reports involving the following: • Alerts (real-time) • Outstanding tickets (customized) • Hourly Ticket Analysis (different time buckets - customised) • Incident Count • Docket Count with ISP - SP-wise and total • Problematic Links Details. • Device configuration changes - CRF confirmation • Average uptime per link in hours - monthly / percentage • RFO Analysis - Resolution Analysis ✓ Top 10 Inbound Utilization ✓ Top 10 outbound Utilization ✓ Top 10 Memory Utilization ✓ Top 10 CPU Utilization ✓ Uptime analysis of the Links ✓ SLA Compliance Report ✓ Capacity Planning Report ✓ Issues & Concerns
8.	IT Security Management	xi. Logs of firewalls/IDS/IPS (daily) xii. Rules of firewalls/IDP/IPS (always updated -to be shared whenever required) xiii. Report of change in security rules in firewalls/IDS/IPS (whenever such change occurs) xiv. Report of security threats with proper identification of the nature (whenever it arises) xv. Vulnerability scan reports (quarterly)

		xvi. Pre-defined compliance report to meet standard compliances (like PCI DSS, ISO 27001 etc.) (whenever required) xvii. Real time notification whenever an user tries to access restricted sites (whenever such case arises) xviii. Real time reporting of active malwares in the network and its mitigation (daily) xix. Statistics of usage of firewall rules (may be required to optimize the rules) (quarterly) xx. Miscellaneous Reports • IPS Report- Daily • Firewall Health status - Daily • Events Report - Daily • Summary of Changes - Daily • The above reports may be consolidated on weekly / monthly / quarterly basis
9.	DBA (Oracle, MySQL and MSSQL)	iii. Report Change of data base users (whenever such thing happens) iv. Change of database schemas (whenever such thing happens)
10.	ITSM Service Provider Management	iii. Log of calls to third party ITSM Service Providers, reasons, measures taken by the 3rd party ITSM Service Providers etc. (daily) iv. Report about performance of each 3rd party ITSM Service Provider (quarterly)
11.	Helpdesk and Service desk Management	viii. Status report of raised/pending/closed concerns by the users (daily) ix. Report about concern escalations, their status (daily) x. List of service ITSM service engineers along xi. with their resume (always updated - to be shared whenever required) xii. Notification about change in service engineers (in advance) xiii. Gate pass issued to visitors (daily) xiv. Inventory of computer stationery and consumables (weekly)

17. ANNEXURE XVI – Tools

ITSM Service Provider should deploy tools but not limited to list

1. ITSM Service Provider has to plan, design, integrate, implement, roll out, manage, migrate the tools for the contracted period.
2. ITSM Service Provider has to document the detailed solution architecture, design, traffic flow etc. ITSM Service Provider should review Bank's existing architecture and on the basis of that provide a solution for integration/implementation of all tools.
3. ITSM Service Provider has to own the responsibility of making the tools run as desired by the bank.
4. ITSM Service Provider shall ensure that during the various phases of implementation, the performance, security etc of the existing network setup is not compromised.
5. if some components are missed out or not properly sized, onus is on the ITSM Service Provider to supply and replace it without any cost to bank.
6. All necessary entitlements, papers of license for software should be provided to bank onsite NBD (next business day) support, back-to-back OEM TAC supports. (24*7)
7. All licenses should be in name of NABARD.
8. The ITSM Service Provider has to design, lay and test the solution to cater to the requirements. The solution has to be deployed at DR DC locations for the bank & any other locations as decided by the bank.
9. The ITSM Service Provider has to submit escalation matrix and keep bank informed, if any changes take place.
10. Design and implementation have to be done by the SI with the support of OEM.(If needed onsite for OEM)
11. All product updates upgrades & patches should be provided by the selected ITSM Service Provider free of cost during the warranty period.

12. ITSM Service Provider should inform Bank about all release/ version change of patches /upgrades/update of software/OS/ middleware etc. as and when released by OEM.
13. ITSM Service Provider should keep the bank explicitly informed about the end of support dates on hardware and software and related products and should ensure support during the period.
14. ITSM Service Provider has to prepare and supply the standard configuration/ backups/compliance/reporting etc. template as per Bank's requirement.
15. All tools will be evaluated for the period of six months and IT Service Provider has obtain sign off from the NABARD for tools.
16. NABARD will evaluate all tools prior to implementation to verify that tools has features and meet specifications are per RFP (with the help of POC). NABARD has right to cancel subscription to any tool, if it does not meet specifications. ITSM Service Provider has to replace tool with appropriate tool as per specifications given in RFP without any additional cost.
17. All tools should be licensed with subscription and support from OEM.

List of tools

1. Desktop Management

The solution should contain following software features:

1.1. Remote device discovery
1.2. Hardware discovery
1.3. Software discovery
1.4. Automated inventory generation
1.5. Remote control utilities
1.6. Security audit data generation
1.7. Audit tracking and action logging
1.8. Task automation
1.9. Patch automation and management
1.10. User account management
1.11. Remote task management
1.12. Desktop migration assistance
1.13. Power management
1.14. Security policy enforcement and remediation
1.15. Wake-on-LAN
1.16. Troubleshooting tools
1.17. Cloud, on-premise, or hybrid deployment options

1.18. Centralized dashboard
1.19. Cloud , on-premise storage options
1.20. SLA compliance tracking
1.21. Software license management
1.22. Third party support and integration

2. Asset Management, Tracking and Inventory Management

The asset management should have following features:

2.1. Asset Lifecycle Management
2.2. Online Inventory Management
2.3. Online Tracking Technologies
2.4. Asset Check-in and Check-out
2.5. Maintenance Management
2.6. Work Order Management
2.7. One Centralised System
2.8. Asset Discovery
2.9. IT Help Desk Management
2.10. Onprem and Mobile-friendly
2.11. Dashboard for all IT assets in Network
2.12. API for data interlinking with NABARD asset management tool
2.13. On demand inventory report generation

3. Ticketing tool

The ticketing tool should have following features

3.1. Asset Management
3.2. Document Management
3.3. SMS and Email Integration
3.4. Customer DataBase
3.5. Live chat system
3.6. Billing & Invoicing
3.7. Surveys & Feedback
3.8. Knowledge Base
3.9. Alerts/Escalation
3.10. Incident Management
3.11. Service Desk (ITIL ITSM)
3.12. Ticket Management
3.13. Help Desk Management
3.14. Problem Management
3.15. Service Level Management
3.16. Service Level Agreement (SLA) Management
3.17. Change Management
3.18. Integration with Application, NMS,Security devices ,SIEM etc

3.19. Ability to generate trouble tickets of various severity on the basis of not running of batch jobs as per schedule

3.20. Ability to generate trouble tickets of various severity on the basis batch jobs running beyond a threshold time

3.21. Generate trouble tickets based on non receipt of extracts from the source systems both internal and external

3.22. Ability to trigger e-mail and sms alerts to specific email addresses and mobile numbers based on occurrence

3.23. Allow users to raise incidents / trouble tickets through email and sms

3.24. Knowledge management system to enable easy resolution of similar trouble tickets by L1 professional

3.25. Identify patterns in the batch jobs - identify jobs that are consistently failing / taking long time to merit further investigation

3.26. Track the resolution of trouble tickets against the service level agreements

3.27. Auto ticketing integration for all authorized devices and enterprise applications used in NABARD.

3.28. Ticketing tool should support application/user specific isolated ticketing and dashboard view.

4. EDR

Endpoint Detection and Response tool should contain following features

4.1 The solution to propose, supply, deliver, install, test, commission and maintain Advanced Endpoint Protection Solution.

4.2 The proposed Advanced Endpoint Solution shall be able to:

4.3 Prevent all exploits, including those utilizing unknown Zero-Day vulnerabilities;

4.4 Prevent all malicious executable, without requiring any prior knowledge;

4.5 Provide detailed forensics against prevented attacks on the endpoint;

4.6 Be effective in preventing Exploits and Malwares without connectivity or updates from Management Server(s) and/or cloud-based resources.

4.7 The Tenderer shall propose the following for implementation in ORGANIZATION environment: Advanced Endpoint Protection (xxxxx Workstations, xxxx Servers, Android Mobile Devices)

4.8 The proposed solution shall co-exist with the existing endpoint security solution. (i.e. Anti-Virus, Host-based Intrusion Prevention Systems, Software Delivery, etc.) in the ORGANIZATION environment in terms of threat and malware prevention.

4.9 The proposed solution must be able to support a wide range of Windows operating systems including Servers 2016, Microsoft October 2018 released

4.10 Redstone 5, Windows 2016 data center, or latest OS.

4.11 The proposed solution must be able to support Windows, MacOS and Linux including, but not limited to Amazon Linux, Oracle linux and Linux Containers etc.

4.12 The proposed solution must be able to support both Workstations, Servers and Android with single license

4.13 The proposed solution must be a signature less solution.

4.14 The proposed solution must be Microsoft Windows Security Center Certified or recognized

4.15 The proposed solution must able to protect proprietary applications such as in-house applications

4.16 The proposed solution must cover the VDI (by VMWARE and Citrix etc).

4.17 The proposed solution must be cloud based management.

4.18 The proposed solution shall have the built-in capability to allow administrator to submit in-correct malware report from the management GUI

4.19 The proposed solution shall have the capability to report all security incidents back to management immediately as long as the endpoint is connected to the management

4.20 The proposed solution shall provide Web-based Graphical User Interface (GUI).

4.21 The proposed solution shall allow customer to purchase additional storage space in the later state or after the solution is operation

4.22 The proposed solution management shall also able to manage policy for mobile (eg. Android) in one single console

4.23 The proposed solution management shall allow user to upgrade endpoint without third party software or tool

4.24 The proposed solution management shall provide malware file report view online or download as pdf.

4.25 The proposed solution management shall provide capability for administrator to create exception directly from security event

4.26 The proposed solution management shall provide 2FA capability without need of customer integration

4.27 The proposed solution management shall provide 2FA without need of separated purchase

4.28 The proposed solution shall provide grouping capability as following but not limit to:
i.Static – select from existing connected endpoints
ii. Dynamic – by defining conditions based on Endpoint name, Domain, IP Addresses, VDI, agent version, and the Operating System on Endpoints.

4.29 The proposed solution shall provide the capability to get intelligence feed from Palo Alto Networks firewall without any additional custom integration or configuration.

4.30 The proposed solution shall provide capability to integrate with on-premises Active Directory

4.31 The proposed solution shall provide capability to forward logs to on-premise SIEM or Syslog server

4.32 The proposed solution shall provide sandbox capability without separate purchase

4.33 The proposed solution shall provide the prevention against exploit kit that do fingerprinting through browser (example: Internet Explorer and Edge)

4.34 The proposed solution shall provide prevention against exploit that attack the operating system kernel through kernel privilege escalation

4.35 The proposed solution shall prevent attacks which change the execution order of a process by redirecting an asynchronous procedure call (APC) to point to the attacker's malicious shellcode

4.36 The proposed solution shall be able to provide real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc.

4.37 The proposed solution must be able to protect the systems without knowing the CVE numbers

4.38 The proposed solution shall prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking through core exploits techniques.

4.39 The proposed solution should provide the capability to perform exploit monitoring and prevention based on core exploit techniques without connection to the Management Server and/or Cloud Service or without relying on signatures.

4.40 The proposed solution shall collect forensic data like process name, file source and path, time stamp, memory dump, operating system version, user ID,

4.41 vulnerable application version while terminate the particular process that under attack

4.42 The proposed solution shall utilize core exploit technique to prevent or block. It shall not be based on signatures or reputation of the file.

4.43 The exploit technique modules shall be able to apply to known and popular applications as well as authorized unknown or in-house developed applications.

4.44 The proposed solution shall prevent dylib hijacking for MacOS

4.45 The proposed solution shall provide protection against exploits including MacOS, Windows, Linux and processes running in Linux Containers.

4.46 The proposed solution shall provide automated forensic memory dump analysis to allow administrators to quickly understand exploit events

4.47 The proposed solution shall also provide Behaviour Analytics capability to prevent or block suspicious activities which may or may not related to exploit

4.48 The proposed solution shall provide protection against malicious DLL files

4.49 The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file

4.50 The proposed solution shall support protection against the execution of malicious executables.

4.51 The proposed solution shall have the capability to restrict files and applications execution on or from local folder, network folder, external media (eg. USB Drive and Optical Media).

4.52 The proposed solution shall have the capability to restrict files and applications from loading another process that is unknown or in the background (a.k.a child processes)

4.53 The proposed solution shall use signature-less type of technology to prevent malware

4.54 The proposed solution shall use dynamic analysis technology(i.e Sandbox) to identify unknown malicious executables including DLL but not limit to

4.55 The proposed solution shall use Machine Learning technology to prevent malware on Windows, Mac OS, Linux, Linux Containerized processes, and Android

4.56 The proposed solution shall have multi-layer prevention technology that include but not limit to sandbox, machine learning and restriction

4.57 The proposed solution shall have the capability to create custom prevention rules based on the behavioural conditions

4.58 The proposed solution shall include cloud sandbox with NO additional cost

4.59 The proposed solution shall have the capability to prevent unknown or zero-day malware when the endpoint is offline (NO internet or management connection)

4.60 The proposed solution shall have the capability to prevent unknown file or application through restriction policy

4.61 The proposed solution shall have the capability to prevent unknown file from execution until the file has been verified.

4.62 The proposed solution shall have the capability to prevent executables file by customer provided hashes

4.63 The proposed solution shall have the capability to identify and prevent greyware

4.64 The proposed solution shall automatically submit unknown file to sandbox without the need of administrator intervention

4.65 The proposed solution shall have the capability to quarantine unknown and zero malware

4.66 The proposed solution shall be able to identify and prevent sophisticated attacks that utilize legitimate processes and actions for malicious activity based on run-time behavior

4.67 The proposed solution should provide disk encryption capability for Windows and Mac platforms

4.68 The proposed solution should provide host firewall capabilities for Windows and Mac platforms

4.69 The proposed solution should provide device control capabilities for Windows and Mac

4.70 The proposed solution should provide rouge device discovery capabilities to detect unmanned devices

4.71 The proposed solution should provide application inventory capabilities across windows, Linux and Mac platform

4.72 The proposed solution should provide vulnerability managed capabilities on linux and Mac platforms.

4.73 The proposed solution shall allow security administrator to hunt using Indicator of Compromise or Combine of multiple behavior of the Indicator

4.74 The proposed solution shall have the capability to display the attack timeline

4.75 The proposed solution shall have the capability to show the suspicious file was loaded or launched by which parent processes

4.76 The proposed solution shall not limit to only endpoint but also able to show and correlate network data from firewall

4.77 The proposed solution shall provide the behavior recording capability like network and user behavior analysis through solution provided sensors and not

4.78 through Netflow data

4.79 EDR, network user behavior analysis and Prevention should be a single endpoint agent

4.80 The proposed solution shall have the capability to blacklist suspicious file from the investigation console

4.81 The proposed solution should have the capability to create custom rules to monitor file integrity changes(FIM).

4.82 The proposed solution should have the capability to monitor file operations

4.83 The proposed solution should have the capability perform enterprise wide search for the file operation like read, write and delete

4.84 The proposed solution shall be able to profile the environment for behavior detection based on but not limited to:

4.84.1. Peer
4.84.2. Time
4.84.3. Entity

4.85 The proposed solution shall be able to detect behavior as following but not limit to:

i.Command and Control
ii. Reconnaissance
iii. Data Exfiltration

4.86 The proposed solution Network and User behavior analysis shall not be based on Net Flow. It shall base on AI or Machine Learning technology with combine of Endpoint, Logs and Networks

4.87 The proposed solution shall be able to detect fileless attack and script base attack without using signatures

4.88 The proposed solution shall provide query builder for threats hunting base on the following but not limited to:

i.Process
ii. File
iii. Hash (MD5 and SHA256)
iv. Network (IP addresses, port, protocol, country)
v. Registry
vi. Signer

4.89 The proposed solution shall be able to provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process

4.90 The proposed solution shall be able to create behavior indicators to identify malicious intent

4.91 The proposed solution shall be able to detect threats on unmanaged device or network anomalies based on peer behavior

4.92 The proposed solution shall have the capability to chain detection from network, endpoint and cloud.

4.93 The proposed solution shall allow administrator to create custom detection rules to adapt based on the environment.

4.94 The proposed solution shall have Live Terminal as a response capability

4.95 The proposed solution shall have Remote Isolation as a response capability

4.96 The proposed solution shall have Process Termination as a response capability

4.97 The proposed solution shall have the capability to assign and track the status of any incident

4.98 The proposed solution shall have the capability to do enterprise wide search and destroy option

4.99 The proposed solution shall have a natively built-in dashboard to monitor the followings of the ORGANIZATION:

a. The Unresolved Security Events in the defined timeframe with different severities
b. The OS platform and the number of managed agents
c. The endpoint license consumption status and its expiry date

4.100 . The proposed solution shall be able to monitor the health of the individual endpoints in the ORGANIZATION, including but not limited to:

a. Endpoint Hostname
b. User
c. Status
d. Underlying OS
e. Agent Version
f. Last Seen Time

4.101 The proposed solution shall provide a high-level summary of the security and deployment status of endpoints. The report can be scheduled to run on a

4.102 recurring basis and on-demand. The report shall be able to optionally send to one or more email addresses.

4.103 The proposed solution shall support the collection of forensic data captured by the advanced endpoint solution to a centralized location.

4.104 The proposed solution shall support automatic collection of the following forensic information for further investigation purposes:

i.Memory Dump
ii. Accessed Files
iii. Loaded Modules
iv. Accessed URI
v. Ancestor Processes

4.105 The proposed solution shall have the capability to view high level system information about the endpoint after the threat has been detected and also

4.106 provide the capability to retrieve the prevention data for further analysis and investigation.

5. SIEM

5.1. The SIEM MUST be able to collect logs in near real-time and start processing as soon as possible.
5.2. The solution MUST have inbuilt ticketing/incident workflow management and integrate with external ticketing system.
5.3. The SIEM solution MUST have built-in evidence locker capability.
5.4. The proposed solution MUST have predefined Use Cases out of the box.
5.5. The SIEM MUST allow the admin to visualize the attack through a simple diagram showing the connection from the source to the destination
5.6. Solution being offered MUST include full packet capture and network forensics capabilities and session replay.
5.7. The proposed solution MUST support structured AND unstructured search (Google type search).
5.8. Solution MUST support incident management and response Solution MUST support user activity monitoring.
5.9. Solution MUST integrate with a LDAP or AD solution for access provisioning to the SIEM system.
5.10. The solution MUST support integration with other security solutions, Patch & Vulnerability Management tools, IPSs, Antivirus, Database Activity Monitoring, etc.
5.11. The solution MUST report on devices that are no longer actively sending logs to the SIEM solution.
5.12. The solution should be able to accepts logs from all industry standard formats (CEF, LEEE, etc.)
5.13. The solution MUST support auto-discovery of assets that are being protected or monitored.
5.14. The solution SHOULD have capability to arrange assets (machines) into groups e.g. Group machines requiring a similar type of configuration e.g. based on OS versions etc.
5.15. The solution must be able to export logs in pdf, html,csv, doc, xls, etc.

5.16. Application Performance Testing

- Synthetic Monitoring, Proactively monitor endpoints with API,
- Real user monitoring
- Database monitoring
- Validate HTTP, SSL, DNS, Web Socket, TCP, UDP, and ICMP from several WAN locations
- Get in-depth insights on the health of your applications running on various platforms like .NET, Java, Ruby, Node.js, and PHP.
- provide network outage timing data for precise RCA
- Verify end to end API calls and HTTP requests
- Automatic discovery and mapping of application and its infrastructure components to maintain real-time awareness in dynamic environments
- End-to-end observability of an application’s complete HTTP/S transactional behaviour to understand the effect on business outcomes and user experience

- Mobile and desktop application monitoring on mobile and desktop browsers to track user experience across platforms
- Root-cause and impact analysis of application performance problems and business outcomes for faster, more reliable incident resolution
- Integration and automation with service management tools and third-party sources to keep pace with an expanding and evolving infrastructure
- Business KPIs and user journey analysis (for example, login to check out) to optimize user experiences and provide transparency into how changes impact KPIs
- Endpoint monitoring to understand how mobile applications impact endpoint devices and identify issues with those devices
- Virtual desktop infrastructure (VDI) monitoring to maximize the productivity of employees using VDI
- URL response

6. Patch Management

6.1. Proposed patch management solution must offer all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating system. The OS may be all the flavours of Windows client OS(Windows 8 and above and all future versions), all flavours of Windows Server OS, all flavours of Linux Server OS, all flavour of UNIX server OS. Guest OS in VMs (Using any hypervisor like VMware/ Hyper V/ Citrix etc.). All critical application/software must also be patched as soon as patch/upgrade is available. Solution must support Intel and AMD CPUs both x86 and x64 architecture.

6.2. Proposed solution should do granular filtering of software patches based on environment requirements.

6.3. Proposed solution should identify, schedule, deliver and track operating system and automate patch delivery.

6.4. Proposed solution should provide end-point security with automated OS and application patch management.

6.5. Proposed solution should remedy endpoint vulnerabilities and enforce security policies.

6.6. Proposed solution should schedule periodic scans computers to identify missing patches

6.7. Proposed solution should identify and download missing patches from vendors' websites.

6.8. Proposed solution should download required patches and create tasks to schedule patch deployments

6.9. Proposed solution should be supported for deployment of patches at end-points and servers

6.10. Proposed solution should provide industry recognized vulnerability scanning and reporting for the purposes of integrated remediation of non-compliance

6.11. Proposed solution should have bundled reporting software so no third party tools would be required to customize reports

6.12. Proposed solution should be able to provide audit reports.

6.13. Proposed solution should be capable of providing Asset Management List with details of all the Hardware and/ or software installed on Bank's network as and when required by the Bank.

6.14. Proposed solution should be capable of integrating with one or more Active Directory structures whenever required

6.15. Proposed solution should have the ability to throttle bandwidth, either statically or dynamically. The throttling capability must support up and down .stream throttling for both the server and agents

6.16. Proposed solution should be capable of using existing client computers as distribution points at remote sites without the need of allocating dedicated servers.

6.17. Proposed solution should support centralized architecture.

6.18. Proposed solution should be able to deploy patch management agent as well as the patches with the help of IP addresses / host name.

6.19. Proposed solution should have the ability to do centralized patch management for PCs, Servers, mobile device like Laptops and Surface Device

6.20. Proposed solution should be able to install package through following mechanisms: Push Pull User self-service

6.21. Proposed solution should support virtualized environment

6.22. Proposed solution should provide remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory or Local Administrator Authentication for deploying agents to remote computers

6.23. Proposed solution should provide easy to use in-place upgrade procedures for all components through the console

6.24. Proposed solution should have native support for high level of encrypted communications without any dependency on additional software, hardware, third party certificates or Certificate Authority

6.25. Proposed solution should support the IPv4 & IPv6

6.26. Proposed solution should support centralized administration, role-based access control and administration without much load on the network

6.27. Latest fixes/ updates should automatically be downloaded to the patch management server on the same day that the patch is made available on software vendors' websites.

6.28. All the patches downloaded must be applied to the endpoints (all devices like servers, laptops and PCs) after successful testing to avoid any disruption in services.

6.29. There should be a UAT set-up where every patch is to be tested before actual installations at endpoints or servers.

6.30. If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from internet, then the integrity of all such content must be verified by the proposed solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the downloaded file is intact and unchanged.

6.31. Proposed solution should be able to determine if a patch has already been installed on a node, even though it is assigned manually. Proposed solution should have the capability to analyse appropriate patches of the OS/ applications for the Desktop/ server in comparison to the latest available patches/ updates released by respective OEMs

6.32. Proposed solution should be able to detect the required patches according to individual node's configuration

6.33. Proposed solution should allow users to postpone the deployment of a patch for a period of time determined by the administrator

6.34. Proposed solution should support event-driven remediation i.e. automatically initiate the process on receipt of a critical patch

6.35. Proposed solution should support rollback of patches and service packs applied

6.36. Proposed solution should have the capability for remediation i.e. continuously deploy, monitor, detect and enforce patch management policies

6.37. Proposed solution should support easy integration with enterprise Wide area Network (WAN) i.e. providing vulnerability assessment, device discovery etc. as per the IP address/host name/ domain

6.38. Proposed solution should be able to deploy any software/ files through the patch management solution

6.39. Proposed solution should have the capability to generate report specific to one group of servers/endpoints or should be capable of generating reports with an enterprise view

6.40. Proposed solution should be able to verify if the patches on desktop are correctly installed by confirming that the vulnerability has been remediated

6.41. Proposed solution should come along with standard reports and should generate customized reports as per business requirement

6.42. Proposed solution should support various reporting formats i.e. reports can be downloaded easily and or exported

6.43. Proposed solution should have the ability to consolidate scan data and to produce a single report for the entire network

6.44. Proposed solution should support regulatory specific reports

6.45. Proposed solution should be able to manually group computers together for deployment of patches. Proposed solution should provide the ability to dynamically group computers based on asset and software information

6.46. Proposed solution should support the grouping of patches into a 'baseline' which can take the form of monthly patch bundle e.g. 'Critical Patches'

6.47. Proposed solution should be able to re-deploy the patch on a computer automatically if the initial deployment is not successful and even if the deployed patch is un-installed by the user

6.48. Proposed solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc

6.49. Proposed solution should come along with all operational technical manuals along with other related documents

6.50. Proposed solution should be able to identify the computers that have installed the patch that is to be rolled back on need basis and rollback updated patches on need basis.

6.51. Proposed solution should be able to provide real-time (within minutes) patch deployment status monitoring

6.52. Proposed solution should allow console operator to deploy patches to all computers via a central console without intervention from the users or allow console operator to target which computers to deploy the patches to

6.53. Proposed solution should allow console operators to spread the patch deployment over a pre-defined period of time to reduce overall impact to network bandwidth

6.54. Proposed solution should be capable of generating reports on patches deployed, when, by whom, to which endpoints, etc.

6.55. Proposed solution should be able to identify systems with non-patched vulnerability conditions

6.56. Proposed solution should allow the console user to deploy actions to remediate against the vulnerabilities identified

6.57. Proposed solution should have the dashboard to drill down to show details for both compliant and non-compliant systems, including but not limited to, noncompliant controls, component name, category, identifier and type

6.58. In the proposed solution, information reported should not be more than 1-7 days old for devices that are active on the network

6.59. The reporting module should contain, but not limited to, the following reports: (i) Progress of all patches applied (ii)Patch Compliance report for selected month /System (iii)Patch Compliance report for single patch (iv) Number of vulnerabilities detected by month; (v) Total number of computers managed and the distribution of these computers;

6.60. Proposed solution should allow console operators to export report in CSV, PDF, XLS & HTML format

6.61. Proposed solution should allow console operators to customize and save the reports without the use of third party reporting tools

6.62. Proposed solution should allow console operators to drill-down from the report to the specific computers

6.63. Proposed solution should allow console operator to trigger alerts when user defined conditions are met

6.64. Proposed solution should generate both pre-packaged and custom, wizard generated reports like compliance reports can be generated for one month patches or one particular patch on all system or on one system

6.65. Proposed solution should be capable of software distribution and installation e.g. Chrome patches, MS Office patches

6.66. Proposed solution should have automatic patch management and deploy patches for various platforms including Windows, Linux, Unix .

6.67. In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals

6.68. In the proposed solution, reports should be viewed online

6.69. In the proposed solution, reports should be downloaded in CSV, PDF, TXT and XML formats

6.70. In the proposed solution, reports should be sent through emails

6.71. The proposed solution should support proper business continuity plan.

6.72. Vendor should provide interface to integrate to multiple monitoring and reporting tools.

6.73. The proposed hardware and solutions should conform to best practices to ensure minimum 99.5% service availability.

6.74. The ITSM Service Provider should have premium support arrangements with the respective OEM. The successful ITSM Service Provider should have back to back agreement with the OEM for Hardware related issues (RMA), troubleshooting, patching, support through call centre or customer web portal and any other services which Bank is entitled to obtain from the OEM. The ITSM Service Provider and Bank should be able to log a call with the OEM directly.

6.75. The successful ITSM Service Provider shall handle all matters including the configuration, implementation, operation, monitoring, management and maintenance of the proposed solution.

6.76. At any point of time, the resource including CPU utilization of any server/ appliance should not go beyond 70%. If the same crosses the threshold of 70%, ITSM Service Provider should replace/ upgrade the hardware to ensure the utilization within the aforesaid threshold without any additional cost to the bank.

6.77. ITSM Service Provider should provide updates, patches, rollups for all software supplied including operating system and should update the same immediately after its release. Back to back OEM support for all Software and updates to current Version is required to be provided. OEM authorization, partner status and back to back support document is to be submitted as part of eligibility bid.

6.78. All critical patches for all software supplied should be applied to end points within 15 days or as per the recommended timeline (whichever is lower) mentioned by OSD/OEM of release of critical patches.

6.79. The proposed solution should be scalable to handle at least 50% above the current requirement.

7. Firewall/NGFW/Router Management Tool

7.1. The solution should be ensuring to clean, optimized, and compliant security controls and network devices. Automate firewall audits to find unused, shadowed, and redundant rules to improve analysis and firewall performance.

7.2. The solution should be able to identify unused rules and redundancies, along with rules that can be simplified, to improve firewall security and speed up troubleshooting. Comprehensive rule life cycle management means that firewall rulesets stay clean.

7.3. The solution should be ensure and demonstrate proper configuration of network devices and security controls in accordance with CIS hardening guidelines and a wide range of compliance standards including PCI, NERC, NIST, FISMA, HIPAA, SOX, and GDPR.

7.4. The solution should Collect and normalize data from all L3 network devices, public and private clouds, software–defined data centers, and OT networks. Correlate all access control lists, security tags, routing rules, NATs, proxies, VPNs, and more. Troubleshoot network connectivity problems and identify root causes.

7.5. The solution should Analyze network configurations, network paths, and application connectivity and access from any source and to any destination. Automate compliance tasks and validate requirements for network configurations, security zone policies, network zones, routers, and switches. Understand policy translations across complex multi–cloud and hybrid network environments.

7.6. The solution should Gain visibility of your cyber risk exposure with end–to–end path analysis across traditional, cloud, and OT networks. Uncover potential attack vectors and reduce your attack surface. Identify vulnerabilities and exposures within your hybrid network infrastructure and mitigate potential exploits leveraging Threat Intelligence.

7.7. The solution should conduct path analysis across hybrid networks, it should analyse network paths and application connectivity from any source and to any destination, detailing devices and rules along the path. Troubleshoot network connectivity and identify root causes of network outages to ensure business continuity and continuous uptime.

7.8. The solution should collects vulnerability data for network security devices (firewalls, IPS/IDS, etc.) and for network infrastructure devices (routers, switches, load balancers, etc.) to ensure that vulnerability analysis and the ensuing prioritization and remediation efforts are effective.

8. PIM/PAM solution

8.1. There should be a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc.

8.2. The solution should be agentless i.e. does not require to install any agent on target devices

8.3. The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection

8.4. The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.

8.5. The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it

8.6. should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric

8.7. authentication server

8.8. The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism

8.9. The solution should also provide local authentication and all the security features as per best standards.

8.10. The solution should provide flexibility user/device wise for local authentication or enterprise authentication

8.11. The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.

8.12. The solution should provide multi-domain feature whereby the entire operations can be carried out within a tenant or line of business.

8.13. The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs

8.14. The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple data center may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations

8.15. The solution shall perform password change options which is parameter driven

8.16. The solution should set password options every x days, months, years and compliance options via the use of a policy

8.17. Ability to create exception policies for selected systems, applications and devices

8.18. The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full

8.19. character set that can be used for passwords on each target system.

8.20. The solution enables an administrator to change a target account password to a random value based on a manual trigger or automatic schedule.

8.21. Allow single baseline policy across all systems, applications and devices (e.g. one single update to enforce baseline policy

8.22. The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')

8.23. Ability to generate 'One-time' passwords as an optional workflow

8.24. Ability to send notifications via email or other delivery methods triggered by any type of activity

8.25. Ability to send notification via email to the user requesting the password that checkout is complete

8.26. Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period

8.27. All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys

8.28. The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities

8.29. The solution should have the ability to reconcile passwords manually, upon demand

8.30. The solution should automatically verify , notify and report all passwords which are not in sync with PIM

8.31. The solution should have the ability to automatically "checkout" after a specific time and "check-in" within a specified time

8.32. The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a

8.33. long iteration.

8.34. The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.

8.35. The solution should be able to control re-prints with adequate authorization

8.36. Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)

8.37. The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests.

8.38. The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end user

8.39. The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM

8.40. The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system

8.41. and end user.

8.42. The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/), front-end database utilities on any combination of target account, group or target system and end-user

8.43. The solution should provide for inbuilt database management utility to enable granular control on

8.44. database access for Sql, my Sql, DB2, Oracle etc.

8.45. The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user

8.46. The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user

8.47. The solution can restrict user-specific entitlements of administrators individually or by group or role

8.48. The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical.

8.49. The solution can restrict target-account-specific entitlements of end users individually or by group or role.

8.50. The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.

8.51. The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.

8.52. System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH

8.53. The solution should be able to support an session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments

8.54. The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh, sql+

8.55. The solution should be able to log/search text commands for all sessions of database even through the third party utilities

8.56. The solution should be able to log/search based on text commands for all sessions

8.57. The solutions should support option for enabling session based recording for all sessions on any combination of target account, group or target system and end-user.

8.58. All logs created by the solution should be tamper proof and should have legal hold

8.59. The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group

8.60. The tool can restrict access to different reports by administrator, group or role.

8.61. The tool generates reports in at least the following formats: HTML, CSV and PDF

8.62. System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts

8.63. The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats (non-editable and encrypted) preferably in any proprietary format.

8.64. The session recording should be SMART to help jump to the right session through the text logs

8.65. Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.

8.66. The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary

8.67. The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording (Optional). All other commands will be included.

8.68. The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including

8.69. accounts that are not managed by the privileged account management solution

8.70. The proposed solution shall allow configuration at platform level to allow selective recording of specific device (Optional).

8.71. The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the

8.72. target machine without exposing the desktop or any other executables).

8.73. The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.

8.74. he proposed system shall support full colour and resolution video recording.

8.75. The proposed system shall support video session compression with no impact on video quality. PIM Security

8.76. All communication between system components, including components residing on the same server should be encrypted.

8.77. All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)

8.78. The Administrator user cannot see the data (passwords) that are controlled by the solution.

8.79. Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).

8.80. Solution should be TLS1.2 and SHA-2 Compliant and can validate FIPS 140 -2 cryptography for data encryption.

8.81. The solution should secure Solution should secure master data records, entitlement, policy data and other credentials in a non-modifiable storage device/process.

9. NMS

9.1. General Requirement

9.1.1. The Solution should provide modular and should not be framework dependent so that required modules can be added in the future to meet growing/changing needs.

9.1.2. The solution should provide ability to support 3rd party integration and have open API/interfaces for integration.

9.1.3. The solution should provide ability to correlate events across the spectrum of infrastructure components and should support events from components including Network, hardware, multiple-platform servers, database, etc.

9.1.4. The solution should provide ability to provide web based management consoles for managing the infrastructure and should use secured protocols for management of servers

9.1.5. The solution should provide ability to support multiple levels of administrative delegation. It should be able to define multiple levels of administrative domains so that each administrator is assigned certain resources for which they are responsible.The solution should provide ability to provide an event

9.1.6. console for the entire environment for event monitoring. Events should be colour coded on the GUI based on severity

9.1.7. The solution should provide ability to capture all events that are being generated across the complete IT infrastructure, correlate them. Solution should have minimum 500GB of storage capacity to store the data/logs/inputs and able to generate the reports based on the data/logs/inputs. The solution should provide ability to generate web based real time reporting and historical reporting of elements in the infrastructure, providing the ability to format and present

9.1.8. data in a graphical and tabular display

9.1.9. The solution should provide the ability of integrating events to automatically create trouble tickets in Service desk system for in time problem resolution.

9.1.10. The solution should support integration with infrastructure management module to monitor various infrastructure elements like Operating System, Storages, Database and virtualization.

9.1.11. NMS and Service desk solution shall include the following components:

9.1.12. NMS / Service desk software licenses.

9.1.13. Required Database software license for NMS and Service desk.

9.1.14. Manual / Automatic replication and synchronization at Disaster Recovery (DR) site and NLS.

9.1.15. Reporting: - Ability to perform event correlation, sending alerts to administrators, realtime and historical analysis with trend and adhoc reporting.

9.1.16. The solution should provide ability to provide standard Dashboards like Infrastructure overview, Network Device Health etc along with Technology Specific Dashboards and Vendor Specific Dashboards for greater insight and visualization.

9.1.17. Ability to get information from the devices so that they can be categorized by criticality, etc.

9.1.18. The solution should provide ability to provide high level summary page dashboards with drill down context pages which is based on assigning the appropriate role for drill down

9.1.19. The solution should provide ability to support easy to write correlation rules.

9.1.20. The solution should provide ability to correlate events into incidents.

9.1.21. The solution should provide ability to monitor data from non-SNMP devices or obtain data from the Enterprise Management System (NMS) for supported network elements

9.1.22. Solution Functionalities

9.1.23. The solution should have the capability to monitor networking issues, conduct event management & configure monitoring all supported networking devices in infrastructure.

9.1.24. The solutions should have Unified multi-technology, multi- vendor device monitoring capabilities.

9.1.25. The solution should provide fault detection & health monitoring of Various Network elements from the device level to the protocol and interface levels. It shall also provide network performance data & threshold based alerts for real time performance monitoring, reporting and historical trending.

9.1.26. The solution must have fault, performance, and traffic monitoring capabilities

9.1.27. The solution should have reporting capabilities & should be able to depict complex networking data through graphical representations & topologic maps.

9.1.28. The solution should analyze and monitor SNMP and non- SNMP data from all Layer 2 and 3 infrastructure technologies

9.1.29. . It should display them in a unified user interface optimized for very high scale visualization, correlation and network problem-solving.

9.1.30. The Solution shall integrate with email /SMS to notify eventsto concerned people with auto escalation as per pre- defined policy.

9.1.31. The solution should provide ability to do fault management of network devices of various vendors. The solution should provide ability to launch in context view through a common interface

9.1.32. The solution should provide ability to provide traffic / percentage utilization, error statistics, etc. through various reports based on the environment monitored.

9.1.33. The solution must be able to retrieve SNMP data and present the same in a single dashboard.

9.1.34. The solution must be able to identify the root cause of the problem and must visually pinpoint single impacting device, as well as other dependent impacted devices preferably in different colours in topology. Proposed fault management should display connecting link between two devices and port labels in same web GUI once clicked on a particular link. If there are multiple links between two devices all the links between two devices and their connected port labels must be visible in same web GUI and provide ability to Identifies configuration changes as root cause of network problems for supported network devices

9.1.35. The solution should provide ability to support bi-directional integration to supported service desk or trouble ticketing system to open and close service desk tickets resulting from any major network failures for supported service desk tool

9.1.36. The solution should provide ability to support WAN MPLS links management over Fast-Ethernet/Giga-Ethernet interfaces. i.e. branches having two MPLS WAN links terminated on Fast- Ethernet/Giga-Ethernet interface. Incase case of primary MPLS link went down(logically) while respective Fast/Giga Ethernet interface remains up, The Monitoring tool should able to identify primary link status & need to generate alert.

9.1.37. The solution should provide Auto Discovery & inventory of heterogeneous physical SNMP enabled network devices like Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.

9.1.38. The solution should support maps grouped by network topology, geographic locations of the equipment’s and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them

9.1.39. The solution must provide intelligent alarms, RCA and Impact Analysis feature for monitoring VPC domains.

9.1.40. The solution should provide the capability to configure polling intervals on a need basis through a GUI tool, to ensure that key systems are monitored as frequently as necessary.

9.1.41. The solution shall identify over-and under-utilized links and assist in maximizing the utilization of current resources. The solution shall provide Performance of Network devices like CPU, memory & buffers ,TOP Talkers ,etc, LAN and WAN interfaces and network segments.

9.1.42. The solution should provide capability to monitor any device based on SNMP v2c & v3

9.1.43. The solution must be capable of monitoring the availability, health, and performance of core networking devices (including Cisco APIC and ACI) including but not limited to CPU, memory, temperature, interface bandwidth utilization

9.1.44. The solution should also provide in a single console, dashboards and reports for Network traffic composition captured from flow technologies for the traffic pattern across enterprise links

9.1.45. Should be able to generate reports based on business working hours and Non business Hours for the selected time frame.

9.1.46. Network Traffic Analysis solution(NetFlow)

9.1.47. The solution must provide the following Flow-based metrics:

- Rate • Utilization • Byte Count • Flow Count • IP hosts with automatic DNS resolution • IP conversation pairs with automatic DNS resolution • Router/interface with automatic SNMP name resolution • Protocol breakdown by host, link,ToS or conversation. • Utilization by bit pattern matching of the TCP ToS field. • AS number • BGP next hop address

9.1.48. Proposed tool must integrate with Central Network Management solution seamlessly for sending alarms and context sensitive reporting and integrate with common portal.

9.1.49. The solution must be capable of providing the following detailed analysis:

a. Top utilized links (inbound and outbound) based on utilization of every link being monitored by every collection device.

b. Top protocols by volume based on utilization of every link being monitored by every collection device

c. The solution must allow date range selection for the reporting period. The solution must also allow the defined custom reports to be saved indefinitely for future use. All reports should be generated and displayed directly by the solution from a common interface.

d. The solution must be able to restrict views for defined users to specific routers, interfaces, and reports.

e. The user must be able to generate reports from the long term database based on specific thresholds defined by the user where the threshold can be compared to rate, utilization or volume of every monitored interface as a filter for inclusion in the report.

f. The solution must be capable of providing the following detailed analysis:

g. Top utilized links (inbound and outbound) based on utilization of every link being monitored by every collection device.

h. Top protocols by volume based on utilization of every link being monitored by every collection device.

i. Top host by volume based on utilization of every link being monitored by every collection device

9.1.50. The solution must automatically populate a list of interfaces exporting Flow traffic to any of its collection devices without user intervention or individual configuration of the reporting interfaces on the solution. The solution must also support manual edit of the automatically polled information.

9.1.51. The solution must provide the ability to group interfaces into functional groups based on any user criteria. The grouping function must allow users to create group names and add interfaces into that grouping for reporting purposes.

9.1.52. The solution must support interface specific report generation for every monitored interface in the network. The network interface selection must also provide a search function that allows the user to search for interfaces based on text based pattern matching of the device name, interface name, description and active status of all interfaces in the list.

9.1.53. The solution must spot potential bottlenecks with color- coded indicators for interfaces that breach defined thresholds and durations

9.1.54. The traffic monitoring solution must help solving performance problems faster using real-time reports and alarms for every interface on the network for the past 30 days with one- minute granularity

9.1.55. The solution must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems

9.1.56. The traffic monitoring solution must provide real-time reports and alarms at one-minute granularity for every interface on the network

9.1.57. The traffic monitoring solution must be designed to retain and access over a year of enterprise-wide flow data with no data roll ups.

9.1.58. Service Desk Management System (Ticketing Tool)

9.1.59. The proposed solution should integrate with all network applications and devices including as Firewall alerts, NAC alerts, ACI alerts etc. It should be comprehensive solution for ticketing services WRT existing network applications/devices.

9.1.60. The proposed service desk solution must provide flexibility of logging, viewing, updating and closing incident manually/automatically via web interface

9.1.61. The proposed service desk solution must provide intelligence of logging and updating incident automatically via web

9.1.62. The proposed Service desk solution should support ITILv3 processes/Or similar like request management, problem management, configuration management and change order management.

9.1.63. Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.

9.1.64. The proposed service desk knowledge tools solution must provide grouping access on different security knowledge articles for different group of users.

9.1.65. Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.

9.1.66. The proposed service desk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.

9.1.67. The proposed service desk solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web, mobile etc.

9.1.68. The proposed service desk solution must allow the IT team to see the Configuration Items (CI) relationships.

9.1.69. The proposed service desk solution must have a built-in workflow engine. The proposed service desk solution must support Non-linear workflows with decision based branching and the ability to perform parallel processing. It should also have a graphical workflow designer for workflow creation and updates.

9.1.70. It should allow IT team to create solution & make them available on the end . user login window for the most common requests.

9.1.71. The Service Desk Solution should be able to create, modify & close incident ticket with information about the cause of incidents & its impact

9.1.72. The Tool should be capable of automating service desk processes, capturing & tracking information & speeding problem solving process

9.1.73. The Solution should be capable of Identifying & Highlighting IT Infrastructure defects & speed resolution time.

9.1.74. The service desk solution should provide the capability to identify duplicate tickets and allow for creating a parent child relationships that clubs all duplicate/repetitive tickets to a parent ticket

9.1.75. The solution should have the ability to log request on behalf on other users and allow users to track the request as if the requestor has initiated the request

9.1.76. The service desk solution should provide the ability to search the across multiple tickets that includes the incident ticket, Problem ticket, Known Error ticket, the solution ticket to find the most relevant solution without having to individually search each source, The solution should store any Logs data upto 6 months of time

9.1.77. The solution should be able to provide insights in the service level associated with each ticket

9.1.78. The solution should provide built-in Dashboards that provide visibility into the service levels maintained by the participating providers

9.1.79. Integration of Service Desk with Enterprise Network Management System

9.1.80. The proposed Network Management Solution must support integration with proposed help desk or trouble ticketing

9.1.81. system such that integration should Associates alarms with Service Desk tickets in the following ways:

9.1.82. Manually creates tickets when requested by Fault Management GUI operators.

9.1.83. Automatically creates tickets based on alarm type.

9.1.84. Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from with with in the network operation console

9.1.85. Maintains the consistency of the following information that is shared between alarm and its associated ServiceDesk ticket including status of alarms and associated tickets and current assignee assigned to tickets.

9.1.86. The system must support seamless bi-directional integration to the proposed service desk solution for trouble ticketing.

9.1.87. SLA's violation on monitored end user response time must open a service desk incident out of the box.

9.1.88. Dashboard showing the alerts based on the severity and requirement

9.1.89. Capable of integrating those alerts to SIEM

9.1.90. Integrating the solution with PIM/PAM for secure access

9.1.91. All the admin related logs to be recorded and sent to SIEM

9.1.92. Allow only AD integration user/admin ID logins and should not support Local user ID's Map Topology

9.1.93. Displays in a logical connection pattern on a map showing the connectivity and relationships

9.1.94. Provision to search specific folder or resources in a view, map to specific background for each level of the network, upload and change icons of devices/background of the network layers

9.1.95. Provides a drill down view, different time scale of important statistics, user friendly names for the devices using alias names

9.1.96. Show the status of the connections based on the dependent connections and the utilization of the links by displaying connection with different width

9.1.97. Provide Geo Map integration to specify latitude & longitude of devices as per branch location

9.1.98. Network Diagram Builder

9.1.99. Provides provision to draw & map user specific network diagram with appropriate icons for routers, switches, firewalls, servers, WLC, AP etc.

9.1.100. Tool should be able to define Primary & back up line connection, so if primary line fails it should switch over to backup line & notify to administrator

9.1.101. The solution should have internal workflow management for approval process or should be able integrateable with ITSM Ticketing tool

9.1.102. Traffic Flow Monitoring

9.1.103. Able to support multiple Flow technologies like Netflow, sFlow, Jflow, Netstream, IPFIX etc.

9.1.104. It should be possible to associate the network traffic to the Hosts / IP addresses, Applications & Protocols in the network

9.1.105. Solution Flow generation capabilities should be capable to handle 1 Mbps to 10gbps interface connections

9.1.106. Solution should be capable of storing all flow records in 1-minute intervals

9.1.107. Tool should allow exporting reports in the format of PDF, CSV and .doc formats

9.1.108. Tool must provide standard KPI reports

9.1.109. Tool must provide standard SLA reports

9.1.110. Tool must provide multiple type of graphs and data table options including Matrix reports

9.1.111. Tool must have option of report wizard to add SQL type report with options like Group by, Order by, Filters etc.

10. IPAM

10.1. General Requirement

10.1.1. The IPAM Solution must support following functionalities:
10.1.2. Create group
10.1.3. Create Subnet
10.1.4. Add subnet to group
10.1.5. Automatically detect devices
10.1.6. Scanning devices in the network
10.1.7. IP address scanning within the subnet
10.1.8. IP address scanning within the group
10.1.9. The solution should support minimum 1,00,000 IP Address with option to expand further in future without adding additional license including IPv4 and IPv6. The solution should be able to integrate with all network components, servers, hardware's, endpoints etc with option to expand in future without additional license
10.1.10. The solution must NOT use software agents or thick clients
10.1.11. The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.
10.1.12. The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.
10.1.13. The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records
10.1.14. The IPAM Solution must provide integration with devices (Switch/Router/Firewall)
10.1.15. Should show
10.1.15.1. IP Details
10.1.15.2. IP Address
10.1.15.3. DNS name
10.1.15.4. Last alive time
10.1.15.5. Status(Used, Unused)
10.1.15.6. Should show Device Details
10.1.15.7. Mac Address
10.1.15.8. Device type
10.1.15.9. Device name
10.1.15.10. Port Number
10.1.16. Admin should be able to give specific access rights to specific user. Admin should be ableto define workflows for IPAM
10.1.17. The IPAM Solution component must perform host discovery using a variety of methods including ping,TCP,ARP,Clear Cache and device OS mapping.
10.1.18. IPAM Solution should provide centralized Inventory reporting showing which device is assigned to which IP address within the network any time
10.1.19. The tool must be able to present the network topology in hierarchical or in tree form.
10.1.20. DNS Resolver – The IPAM Solution tool must provide the host name of any node whose IP Address is known and vice versa with additional details like

the default net mask, network type, and the status for the forward and reverse lookups

10.1.21. The tool must have the capability to find free address space across a range. In cases where an IP is not used in the network, the tool must prompt that the system does not exist in the network.

10.1.22. The tool must offer quick search capabilities

10.1.23. The IPAM Solution must support splitting and joining of networks to make them smaller and larger – with IP definitions remaining intact

10.1.24. The IPAM Solution shall have adequate security tools to avoid any unauthorized access to the system in particular and solution as a whole. Integration with Radius/TACACS+ and AD for

10.1.25. authentication

10.1.26. The IPAM Solution shall support appropriate logging functionality on itself as well as on external source like Syslog servers

10.1.27. The IPAM Solution shall support one-click system-wide software patching and upgrades wrt to solution.

10.1.28. The IPAM Solution must support hardened OS, available on

10.1.29. physical or virtual appliances, to reduce vulnerability of network attacks

10.1.30. The IPAM Solution must support web administration via secure SSL web interface

10.1.31. The IPAM Solution must support remote login using SSH

10.1.32. The IPAM Solution shall have adequate security tools to avoid any unauthorized access to the system in particular and solution as a whole

10.1.33. The IPAM Solution should have high availability with DC & DR architecture.T he database Synchronization between DC & DR should be automatic with exception for manual control (if required in some cases)

10.1.34. Solution should have the ability to discover Layer 2 and Layer 3 network topology relationships between devices to ensure configuration settings match

10.1.35. Should support different mode for device discovery including CLI, SNMP

10.1.36. Solution should be able create reports be generated in different formats. (PDF, DOC, XLS and HTML formats)

10.1.37. IPAM Solution should provide centralized Inventory reporting showing which device is assigned to which IP address within the network at any time.

10.1.38. Solution should have the ability to add network devices into inventory via auto-discovery. The proposed infrastructure should able to discover n number of devices

10.1.39. User and End Tracking and Port Analysis

10.1.40. Solution should offer infrastructure device port consumption tracking

10.1.41. Can a user display port usage history

10.1.42. Solution should offer end host/MAC address location identification and tracking

10.1.43. Solution should offer end host/MAC address location history and auditing

10.1.44. Solution should report on new and no-longer-present devices on the network

10.1.45. Solution should highlight location and status changes of devices and interfaces

10.1.46. Dashboard showing the alerts based on the severity and requirement

10.1.47. Capable of integrating those alerts to SIEM

10.1.48. Integrating the solution with PIM/PAM for secure access

10.1.49. All the admin related logs to be recorded and sent to SIEM

10.1.50. Allow only AD integration user/admin ID logins and should not support Local user ID's

11. APT

11.1. General Requirement

11.1.1. Should provide the functionality, in real time, to filter the crash results based on multiple dimensions such as app version, OS type, OS version, device- type, jailbroken status, symbolicated and de- obfuscated stack traces with detailed user device information, including steps that led to crash.

11.1.2. Should Monitor, in real-time, everything coming to and from the application.

11.1.3. Should highlight the performance problems that carry adequate actionable information, such as the suspect KPI or problem layer (Web, App or DB) to enable faster MTTR (Mean Time to Restore) as well as faster MTTI (Mean Time To Isolate).

11.1.4. Should provide full visibility into all the activities from web and mobile application user across all devices, browsers and geographic locations.

11.1.5. Should be a transaction- based monitoring and use analytics to track the performance of internal service providers.

11.1.6. Should have the capability to use machine learning based methods to automatically detect anomalies without requiring rule-based configurations or manual thresholds-based methods.

11.1.7. Should be able to give full visibility of customer experience across the digital transactions from the frontend to the backend including various interfaces for the transactions. Should match the functionalities of the existing APM tool of the Bank and provide detailed user journe

11.1.8. Should provide visibility into W3C navigation timings, for user interaction where performance is not satisfactory, and based on the end user browser it should be able to understand the available metric to help understand time spent in browser or network or server.

11.1.9. Should clearly project the problem caused by the JavaScript was due to incompatibility of browser or JavaScript code error.

11.1.10. Should be able to monitor all the components / applications with only the read privilege and without requiring “root” privilege on the monitored application as well as to perform the day- to-day activities of the monitoring solution.

11.1.11. In which the maximum resource utilization of the monitored host, at any time during the day, (by the monitoring solution, in terms of compute) should not exceed 5% of the monitored systems, irrespective of the number of agents installed for monitoring.

11.1.12. Should support fully automated monitoring of addition / removal of VMs/JVMs/Web Servers/IIB processes and queues etc. based on changing load patterns/processes without manual intervention. (for already monitored application)

11.1.13. Should automatically discover and monitor various environments (like Java application servers automatically grouped based on type Tomcat, WebSphere, WebLogic, Glassfish, JBoss, message broker, MQ, database, etc.) without manual intervention like need to select or configure JMX metrics for a selected application process.

11.1.14. Should be able to provide online auto analysis to identify which component or tier is contributing to slowness of the monitored transaction.

11.1.15. Should provide detailed stack trace view of abnormal transaction right from web server through the app server, middleware all the way to the database. Stack trace should include calls made to the 3rd party systems.

11.1.16. Should automatically baseline metrics/KPIs in the monitored environment. Any deviations to this baseline should be automatically correlated so that a single actionable alert can be raised to the respective team.

11.1.17. Should be able to automatically detect the database performance and its impact on transaction performance.

11.1.18. should be able to provide same monitoring functionality for Containerized / Dockerized applications that is available for noncontainerized applications. It should provide container centric monitoring perspectives on Containers / Docker images, services, and hosts.

11.1.19. In which Configuration and management should be through a single, web-based user interface

11.1.20. In which Data in transition and Data at rest should be encrypted.

11.1.21. Should have easy upgrade paths across both major and minor releases, requiring minimal manual configuration edits.

11.1.22. Should be able to automatically learn all the traffic patterns and baseline them. And when anomalies are detected within these patterns, it should be able to alert the operations team

11.1.23. Should provide feature to create custom reports & dashboards.

11.1.24. Should support all major software like IBM WAS, IIB, MQ, IBM IHS, Oracle OHS, TOMCAT HTTP Server,

11.1.25. WebLogic, Oracle DB, .NET etc

11.1.26. Should support for all major OS platforms like Windows, AIX, Linux, Solaris etc.

11.1.27. Should support monitoring of all standalone java, C, Node.JS, AngularJs, etc. programs as well.

11.1.28. Should be capable of working on cloud as well as on prem.

11.1.29. Should support both agent- based and agent-less monitoring.

11.1.30. Should support On-Premise deployment, and none of the bank asset (other than internet-based links) will be exposed to the external world

11.1.31. Should provide complete topology on the spread of infrastructure for an application

11.1.32. Should provide information at the blockages in requests processing

11.1.33. Should provide resource consumption pattern within the resources of VMs allocated at OS level

11.1.34. Should have Cloud monitoring capabilities

11.1.35. Should support Monitoring of Micro services

11.1.36. should be able to automatically detect any deployment changes which may have happened in the application code and correlate that with the any performance issue.

11.1.37. Should be able to auto discover the new instances of batch processes and monitor them in real-time. The solution should be able to pin-point the exact cause of failure.

11.1.38. Should be able to integrate with the various tools of the Bank, including ITSM (BMC) and must be able to share the logs with the SIEM & ITSM System.

11.1.39. Should have an early warning system mechanism. During peak hours it should auto-detect problems before they can impact the customers. The solution must be capable of identifying performance issues and prioritize it.

11.1.40. Should allow to store information for each team and also give role-based access to each user.

11.1.41. Should be able to auto- instrument (means, post- installation of the agent, it should auto-discover) the applications and middleware (web and app servers, IIB and Messaging Queues etc.).

11.1.42. Should be complied with all the data privacy norms as per laws applicable in India. The tool should comply with the future Indian Laws as and when made applicable with-in the stated timeframe. PII data should be encrypted, if part of log.

11.1.43. Should have gone through proper testing against Code Reviews, Penetration Testing, and Open Source risk management. The bidder should be able to furnish appropriate

11.1.44. Compatible with major NABARD applications eg. ECM, CLMAS, FAMS, Ensure, Empower etc.

11.1.45. Should be able to generate load for 5000-10000 parallel sessions, script recording and creation, simulation load model , load generator, test suite automation, real device testing etc

11.1.46. Session replay and root cause analysis of struggling users from replay window

11.1.47. Root cause analysis and rill down capabilities across layers - client / browser side, server, database

11.1.48. Ability to capture client-side / browser-side events (js errors, client-side errors and events) and trigger alerts

11.1.49. Drill down capabilities from funnel exits as well as custom or user configured events

11.1.50. Should have Software Suite for Performance Engineering with Performance Testing, Test Suite Automation, Real Device Testing, Real Browser User Testing, Server Monitoring, Application Monitoring, Database Monitoring

11.1.51. Log Monitoring, User Experience Management

12. SECURE NETWORK CONFIGURATION AND CHANGE MANAGEMENT

12.1. It should be able to auto-discover Physical / Virtual/ software blade network devices across WAN/LAN

12.2. During subsequent discoveries, the solution should be able to identify and alert whenever any new devices added or removed

12.3. Apart from autodiscovery, there should be option add/delete device manually/ through CSV/through API

12.4. it should be integrated with to be proposed NMS solution to be purchased through this RFP.

12.5. It should be capable to discover inventory be used for vulnerability and End of life/End of support devices.

12.6. Capable of configuration/policies/OS images/patches deployment/roll back to multiple devices at a time

12.7. In real time, detect configuration and asset information changes made across a multi vendor device network, regardless how each change is

12.8. made.

12.9. capable to detect, compare & alert on changes based on which

12.10. decision could be made for roll back or implementation of changes with single click

12.11. The device MUST support roll back to a previous configuration & should maintain previous versions and/or configurations

12.12. it should support multiple commands with multiple parameters at a time for individual location to perform task. The solution should be able to perform such tasks in multiple locations at a time.

12.13. The solution should support configuration deployment/roll back using ad- hoc commands, configuration templates or scripting

- **a.** A solution should have provision to schedule the tasks for specific date, weekly, monthly, quarterly etc.& in case of any maintenance window.
- **b.** capable to automate all repetitive and time-consuming tasks related to network devices configuration and change process.

12.14. It should automate routine network operations.

12.15. The solution should be able to track and detect any configuration changes and alert accordingly.

12.16. Detect out of band configuration changes and trigger a configuration back up. Apply configuration changes to device configurations.

12.17. The solution should provide option to schedule the Backup process.

12.18. It also should take care of comprehensive network configuration back up and recovery of all network devices

12.19. It should deploy and monitor IOS operating system images, network security patches from a centralised network management system

12.20. Able to push standard template for new deployment

12.21. there should be reusable template for single and bulk changes

12.22. Automatically identify device vulnerabilities and upgrade the firmware

12.23. In case device itself fails, must generate alert, should not hamper Any production traffic by any means & functionality should swiftly shift to secondary device which could be in same and different location based on the requirement.

12.24. The solution must have an on-device programmable API (NETCONF or REST) that allows an external script to: Get device configuration, Get optional data, change device configurations

12.25. The device MUST return operational data as semi structured (JSON and XML format) not as test print out form of JSON and XML envelops

12.26. The device should return its configuration in semi structured format (JSON

12.27. and XML) with meaningful structure. (for Example ACL line should be within the ACL)

12.28. The device must support replacing current configuration with a new configuration without a reload.

12.29. The solution should be able to create a list of configuration commands needed to transform one configuration into the other

12.30. there should be provision of finding a new network devices as per compliance standard.

12.31. It should have ability to discover Layer 2 and Layer 3 network topology relationships between devices to ensure configuration settings

12.32. It should be capable of automatically generate a script from a list of command line that are input by the user.

12.33. It should be capable of different alerts to be defined as different level of severity or urgency (for example critical, severe or warning)

12.34. Tool Has device communication protocol support like Telnet, SSH, TFTP, FTP etc

12.35. There should not be any limit to the number of concurrent users (operators) accessing the product

12.36. Able to correlate to problem detection, policy violations and topology relationships which help us rapidly identify the likely root cause of network problems

12.37. Back up data can be accessed if the NCCM tool is down or disaster occurs.

12.38. The solution should have ability to perform a textual configuration search using regular expression pattern matching

12.39. The solution should have ability to upload entire achieved configuration files to network devices

12.40. The solution may facilitate a bare metal installation, including initial load of a devices OS software

12.41. Compliance

12.42. the solution should maintain policy compliance using continuous configuration auditing and remediation

12.43. It should ensure that the devices are configured and operating in compliance with regulatory standards

12.44. It should automate audit cycles with built in compliance report and close the loop on compliance with integrated change management

12.45. It provides strategic integration with companywide configuration & change processes & having compliance visibility across all network infrastructure from a single dashboard

12.46. In real time, store a complete audit trail of configuration changes (hardware and software) made to network devices including critical change information

12.47. It should gather data on compliance to policies as a feedback mechanism to drive improvement & capable of compliance reporting. Manage network compliance by comparing devices to custom defined,

12.48. It should be capable of automatic remediation to bring the device back to policy compliance or to a default configuration status

12.49. It should complete operational, security & regulatory policy definition and enforcement

12.50. It should ensure Intelligent remediation of policy violations. Auditing full configurations.

12.51. Management

12.52. It should configure granular, customizable user roles to control permissions on device views, device actions and system actions

12.53. Able to manage device access and authorization through a centralized control model that is integrated with standard workflow and approval processes through mail notifications

12.54. Integration with TACACS, AD , LDAP for centralized group/ role/user management is required

12.55. The solution should be able to integrate with Any market leading Network monitoring solution apart from the mentioned one in this RFP.

12.56. The solution should be integrate with all market leading VAPT tools and automate the task initiation for reported vulnerabilities

12.57. The solution should be integrate with market leading SIEM, SYSLOG tools

12.58. The solution should be integrate with existing/other market leading Incident management and ticketing tool

12.59. The solution should have option to back up the tool configuration

12.60. Track all action according to group /role/ user levels

12.61. Should have provision to get feeds from OEM with regards to releases (version and patch) and notify bank

12.62. Reporting

12.63. There should be a browser based customizable Executive dashboard widget/page showing device statistics & their compliance

12.64. Schedule and generate custom report on all aspects of network device statistics & their compliance

12.65. Schedule and generate custom report on all aspects of network device configuration and change management

12.66. Reports are quickly made and brought together when upper management needs help in making important decisions on capacity additions/device upgrade/SLA verifications

12.67. Able to provide summery notification i.e. daily summery notification option which accumulate all the applicable alert conditions into a single notifications, sent once a day (or other configurable time window).

12.68. Reports can be retrieved in user friendly formats like XML Excel CSV PDF etc.

12.69. Reporting on role based.

12.70. All changes logged and generate in report & Ad-HOC reporting like A)help in audit compliance by comprehensive documentation and reporting. (B)Archive with recording of activities performed. C) Allow to generate report in detail in Task output analysis, patch compliance, security and regulatory compliance, operational compliance, configuration differences, how many configuration updates are performed between certain time across all devices, which operator performs configuration update on which devices, the number of unauthorised updates and polices violations detected and prevented.

13. Application Management Tool

13.1. Performance experienced by end users (both front end and back end) of the application., Performance metrics measures the computational resources used by the application for the load, indicating whether there is adequate capacity to support the load, as well as possible points/locations of a performance bottleneck.

13.2. Monitoring to meet the three functional dimensions of digital experience monitoring (DEM); application discovery, tracing and diagnostics (ADTD); and application analytics (AA).

13.3. Applying data-driven analytics and ML technology to enhance the effectiveness of monitoring.

13.4. Compatible with major NABARD applications eg. ECM, CLMAS, FAMS, Ensure, Empower etc.

13.5. Should support following features:

13.6. Apex Threshold

13.7. Sampling Factor

13.8. Transactional tracing

13.9. CPU time per transaction

13.10. Memory allocation per transaction

13.11. Capture HTTP Parameters

13.12. Background transactions

13.13. Custom Instrumentation using Java Annotations

13.14. Context based monitoring

13.15. Monitoring JMX metrices

13.16. Monitoring Java Agent API

13.17. Support for Tomcat, jBoss

18.Annexure XVIII – Pre Bid Query Format

ITSM Service Provider Name:
Contact Person:
Contact no. / Email Id:

Sl No.	RFP Reference Page No.	RFP Clause No	Existing Clause Details	Clarification sought
1				
2				
3				

19. Annexure XIX – Change Management Process

Introduction:

The change management is the sequence of steps or activities that a change management team or project leader follows to apply change management to a change in order to drive individual transitions and ensure the project meets its intended outcomes.

Objective:

This document provides an overview of the requirements involved in introducing changes for existing systems. It establishes a common approach for requesting, authorizing, executing, testing and implementing the change requests, while maintaining appropriate audit trail.

Scope:

The Change Management is applicable to all systems that are managed by the IT team of Bank. Change Management is required for:

1. Implementing approved changes efficiently, within planned downtime, without disruption to the existing services and with acceptable risk to the existing and to the new IT Services;
2. Preventing unauthorized changes getting implemented in production environment;
3. Supporting new project implementations;
4. Resolving process malfunctions;
5. Supporting continual business process initiatives.
6. This process shall be used for all changes including Incidents, Internal Audit, Management Reviews and other Reviews, Customer & Legal Requirements (but not limited to):
7. New system or software implementations;
8. Customizations and modifications to systems;
9. Upgrades to existing systems or software;
10. Application changes (e.g. functionality updates, web page additions/deletions, URL link additions/deletions, releases, Interface changes etc.);

11. Database changes;

12. System configuration changes in servers (DB, Unix and Windows);

13. Networking changes (Architectural, configuration);

14. Technical Upgradation (Patches, Update, Hotfixes for systems and network devices);

15. Installation, deployment and modification of tools (hardware devices, business, security and management tools);

16. Storage related changes;

17. Changes in business continuity plan;

18. Day to day operational changes for smooth functioning of respective services/activities.

Consequence Management & Non-Compliance:

All violations of this process are subject to disciplinary action. The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from a verbal reprimand, to termination of employment/contract and/or legal action.

If a department or function is unable to comply with any requirements detailed within this process, an exception shall be obtained. Such exceptions shall be documented, indicating the rationale for the exception and the related risks. Exceptions to this process shall follow the exception management process for prior authorization and approval. Any exception to this process has to be duly approved by the CTO.

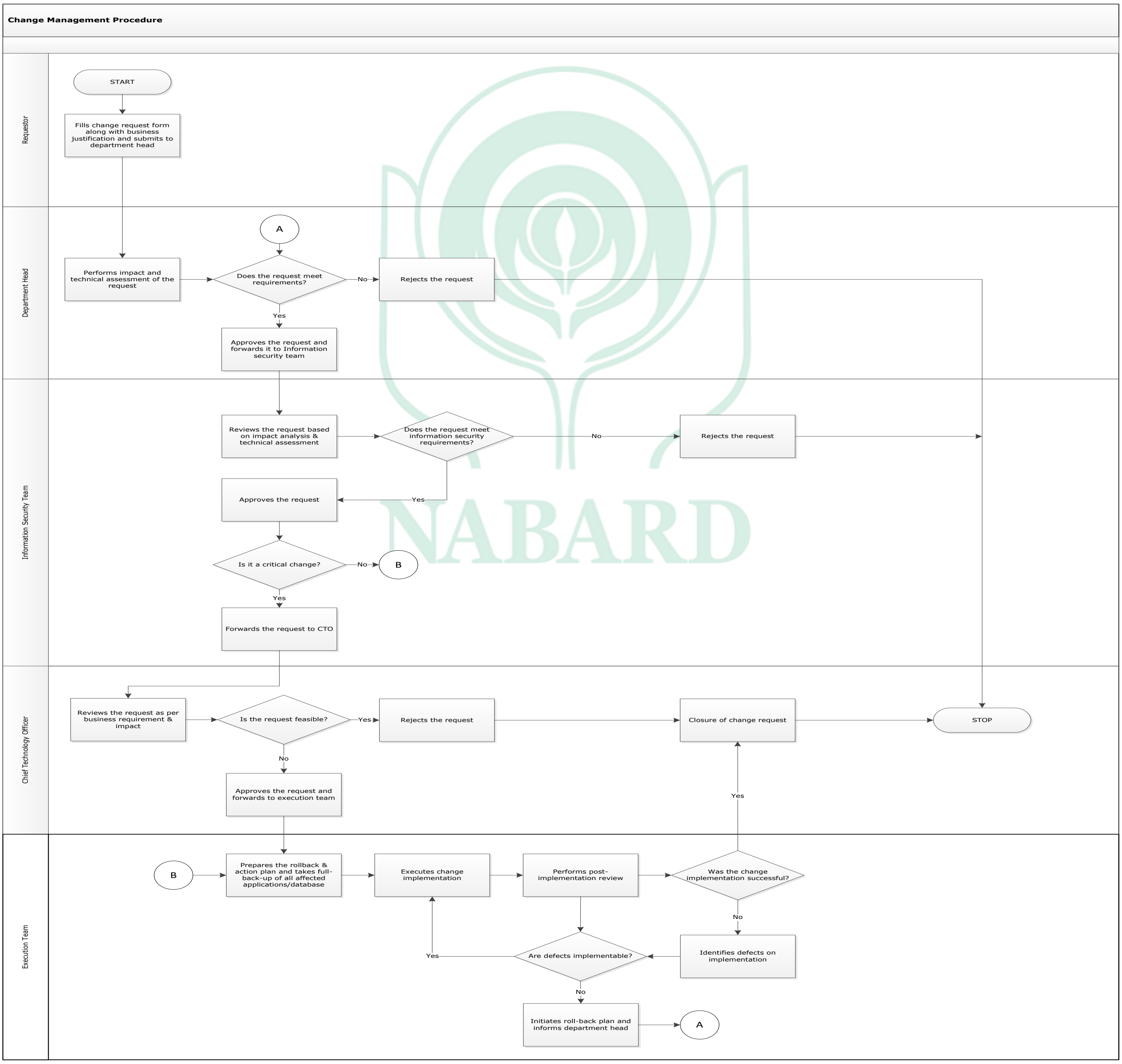
Change process:

All changes to IT services shall follow a standard process to ensure appropriate planning. Changes shall be categorized as an Emergency change or non-emergency change (as mentioned in section 6.1 and 6.2). Appropriate processes and levels of review shall be applied to each type of change commensurate with the potential of the change to disrupt university operations. It is the responsibility of the Change Authority to ensure that all areas under their direction have documented processes that meet minimum standards, are reviewed annually, and are communicated to staff.

Change Request Process:

A change requirement is generated due to a business need, incident/risk mitigation etc. They are generated as part of existing or new projects/applications that are supporting the business needs. Some change requests are also generated as a part of the day to day IT operations and are required for smooth functioning of the activities within the IT operations. Project/application related change requirements shall have a management approval process and that acts as the source for the change request procedure.

Change Request Process Workflow


Change Management Procedure
Requestor
START
Fills change request form along with business justification and submits to department head
Department Head
A
Performs impact and technical assessment of the request
Does the request meet requirements?
No
Rejects the request
Yes
Approves the request and forwards it to Information security team
Information Security Team
Reviews the request based on impact analysis & technical assessment
Does the request meet information security requirements?
No
Rejects the request
Yes
Approves the request
Is it a critical change?
No
B
Yes
Forwards the request to CTO
Chief Technology Officer
Reviews the request as per business requirement & impact
Is the request feasible?
Yes
Rejects the request
Closure of change request
STOP
No
Approves the request and forwards to execution team
Yes
Execution Team
B
Prepares the rollback & action plan and takes full-back-up of all affected applications/database
Executes change implementation
Performs post-implementation review
Was the change implementation successful?
No
Identifies defects on implementation
Are defects implementable?
Yes
No
Initiates roll-back plan and informs department head
A

Non-Emergency Changes:

The requestor will fill the change request form and submit it to the Technical Advisory Board (TAB) with an RFC for review.

The TAB consists of members from the technical teams

The TAB will review and will take the decision to approve or reject the change request for further submission to the Change Advisory Board (CAB) or Emergency Change Advisory Board (ECAB).

CAB and ECAB consists of members from the Business Function, Information Security (InfoSec) and IT team. The change requestor will present the justification for the change.

InfoSec team will review the request as per the information security requirements and will reject or approve the request. If the change is categorized as critical. The change request will be forwarded to the Chief Technology Officer (CTO)

The CTO can approve or reject the change request as per the business requirement and impact. If the request is approved, the change requestor will inform the execution team. (Execution team should be informed by authorized person or committee)

The respective change executing team based on the requirements received, will prepare the change documentation i.e. complete plan of action, impact analysis and rollback plan with proper testing done in the available test environments.

The execution team will assign the appropriate risk assessment category taking into account the impact in the event of failure of the change upon implementation as per the following definitions:

Critical: Changes that affect the internal/external customers/end-users (downtime of services).

Moderate: Changes that do not directly impact the customer/end-user services. These changes may involve addition of new Hardware/software to the infrastructure, customizations without requiring downtime.

Low: Changes that are not meant to have any service disruptions and involves day to day operational activities

Change Types defined with designated approver

	Approver	Operational Day to Day	Impact on Services	New Hardware and Software	Downtime required
Critical	CGM	No	Yes	Yes	Yes
Moderate	CAB	No	No	Yes	No
Low	CAB (blanket approval)	Yes	No	No	No

Before the implementation of the change, the full back-up of all affected applications/database, asset must be taken before copying the changed programs to production or live environment to avoid any eventuality

Post implementation, review is performed by the implementation team by documenting the answers to the following questions in the change request tracker:

Was the change implemented successfully?

Did the change meet the desired results?

Was the change implemented in time?

Was any information missing, which was needed to make a decision at any stage of the process?

Was there any business impact after change execution?

The final authority for closure of change request lies with CTO

If the change executed was unsuccessful, the executing team will initiate the roll back plan. The executing team will also identify the root cause for unsuccessful implementation of the change request and will share the report with the respective department head

All the post implementations change reports must be reviewed by the respective department head

Emergency Changes:

For emergency changes, necessary approvals are sought from the ECAB and the documented process is followed post-facto with all the necessary steps followed as per the documented process for record purposes.

Note: The post-facto steps to be followed using the change request form in case of emergency changes need to be completed within 3 days from the day when the required change was done with necessary approvals sought verbally.

20. Annexure XX – Handover

Incoming ITSM Service Provider will be repressible for taking over following from existing ITSM Service Provider:

Set of all infrastructure handover documents (e.g. detailed and updated HO and RO infrastructure diagram, network diagram, all device and servers admin and user passwords, etc) and their current location along with the latest ITSM symphony database file.

- All RO state wise - updated list of hardware including desktops, laptops, servers, switches, modems, firewall, spare devices, wifi, etc.
- HO - updated list of hardware including desktops, laptops, servers, switches, modems, firewall, spare devices, wifi, etc.
- DC - updated list of hardware including desktops, laptops, servers, switches, modems, firewall, spare devices, wifi, etc.
- DR - updated list of hardware including desktops, laptops, servers, switches, modems, firewall, spare devices, wifi, etc.
- Updated List of software dumps, CD, DVD, pendrives, HDD, backup HDD, etc used by support executives at all locations (HO/RO/DC/DR) along with their critical associated information.
- AMC/Warranty details of all hardware including desktops, laptops, servers, switches, modems, firewall, spare devices, wifi, etc at all locations (HO/RO/DC/DR) with all related documents.
- List of all service providers and their contact number, person, email and escalation matrix.
- All latest user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures etc.
- List of all RCA done during service period.
- All server logbook including windows, linux, AIX etc with all action performed on servers till date individually.
- Knowledgebase of Nabard Infrastructure.
- Updated list of Softwares.
- Updated list of all licenses along with expiry dates.
- List of all approved change requests processed during service period.
- List of backups with description.
- ILL / MPLS configuration details of all connections at all locations.
- Software inventory.
- HLD and LLD of DC, DR, HO, all RO.
- Backup location of all configuration and setting backups of devices/servers/clusters etc.
- Anything not listed above.

21.Annexure XXI – Glossary

Sl No.	Abbreviations	Description
1.	AMC	Annual Maintenance Contract
2.	CAB	Change Approval Board
3.	CTO	Chief Technical Officer
4.	CISO	Chief Information Security Officer
5.	CVC	Central Vigilance Commission
6.	DBMS	Database Management System
7.	DC	Bank's Data Centre
8.	DD	Demand Draft
9.	DDMs	District Development Managers
10.	DIT	Department of Information Technology
11.	Comprehensive IT Services mangement	IT Services Management Solution
12.	DR	Disaster Recovery
13.	DW	Data Warehouse
14.	EMD	Earnest Money Deposit
15.	ECAB	Emergency Change Approval Board
16.	IDAM	Identity and Access Management
17.	InfoSec	Information Security
18.	IT	Information Technology
19.	IEM	Independent External Monitors
20.		
21.	KPIs	Key Performance Indicators
22.	LD	Liquidated Damage
23.	MPLS	Multiprotocol Label Switching
24.	MSME	Micro Small & Medium Enterprises
25.	NABARD	National Bank for Agriculture and Rural Development
26.	NABCONS	NABARD Consultancy Services
27.	NABFINS	NABARD Financial Services

Sl No.	Abbreviations	Description
28.	NABFOUNDATION	NABFOUNDATION
29.	NABKISAN	NABKISAN Finance Limited
30.	NABSAMRUDDHI	NABSAMRUDDHI Finance Limited
31.	NABSANRAKSHAN	NABSanrakshan Trustee Company Private Limited
32.	NABVENTURES	NABVENTURES
33.	OEM	Original Equipment Manufacturer
34.	OFDD	Off Farm Development Department
35.	PBG	Performance Bank Guarantee
36.	PO	Purchase Order
37.	PSU	Public Sector Unit
38.	RBI	Reserve Bank of India
39.	RFP / RfP	Request for Proposal
40.	RIDF	Rural Infrastructure Development Fund
41.	RMD	Risk Management Department
42.	RO	Regional Office
43.	SDLC	Software Development Life Cycle
44.	SDWAN	Software Defined Wide Area Network
45.	SHG	Self Help Group
46.	SI	System Integrator
47.	SIEM	Security information and event management
48.	SLA	service level agreement
49.	SOC/NOC	Security Operations Centre/Network Operations Centre
50.	SPPID	Strategic Planning and Product Innovation Department
51.	TAB	Technical Advisory Board
52.	SQL	Structured Query Language
53.	VAPT	Vulnerability Assessment and Penetration Testing
54.	VPN	Virtual Private Network

APPENDIX I - NABARD Offices – Locations and Addresses

Sr No.	Address	City	Staff Strength			
			Group A	Group B	Group C	Total
1	NABARD Complex, Kamaraj Road (VIP Road), Junglighat (P.O), Port Blair-744103, Andaman and Nicobar	Port Blair	5	3	2	10
2	The Chief General Manager, R.T.C , X Road Musheerabad ,Hyderabad – 500020, Andhra Pradesh	Hyderabad	63	15	5	83
3	The Deputy General Manager, NABARD Bank, Tinali VIP Road Post Box No. 133 Itanagar – 791 111, Arunachal Pradesh	Itanagar	11	4	2	17
4	The Chief General Manager, NABARD, P.O.Box No. 1 Opposite Assam Secretariat G S Road, Dispur Guwahati – 781 001, Assam	Guwahati	55	15	19	89
5	The Chief General Manager, NABARD, Maurya Lok Complex Block B 4 and 5 Floors Dak Bunglow Road Post Box No. 178 , Patna – 800001 , Bihar	Patna	68	20	10	98
6	The Chief General Manager, NABARD, 1st Floor, Pithalia Complex Fafadih Chowk, Opp. Trunk Exchange K K Road ,Raipur - 492009 Chhattisgarh	Raipur	46	12	5	63
7	The Deputy General Manager, NABARD, Nizari Bhavan Menezes Braganza Road Panaji - 403 001	Goa	8	4	0	12

	Goa					
8	The Chief General Manager, NABARD, NABARD Tower, Opp. Municipal Garden Post Box no. 8 Usmanpura Ahmedabad - 380 013 Gujarat	Ahmedabad	78	21	12	111
9	The Chief General Manager, NABARD, Plot. No. 3, Sector 34-A Post Box No. 7 Chandigarh – 160 022 Haryana	Chandigarh	56	17	8	81
10	The Chief General Manager, NABARD, Block No.32 S D A Commercial Complex Dev Nagar, Kasumpati shimla – 171 009 Himachal Pradesh	Shimla	33	10	6	49
11	The General Manager, NABARD, B II, 4th Floor, South Block Bahu Plaza Post Box No. 2 Jammu – 180 012 Jammu & Kashmir	Jammu	36	12	6	54
12	The Chief General Manager, NABARD, Opposite Adivasi College Hostel Karamtoli Road Ranchi - 834001 Jharkhand	Ranchi	57	17	4	78
13	The Chief General Manager, NABARD, NABARD Towers 46, Kempe Gowda Road Bangalore - 560009 Karnataka	Bangalore	76	27	7	110

14	The chief General Manager, NABARD, Post Box No 5613 Punnen Road, Statue Thiruvananthapuram – 695 039 Kerala	Thiruvananth apu ram	49	19	7	75
15	The Chief General Manager, NABARD, E-5, Arera Colony, Bittan Market Post Office Ravishankar Nagar Post Box No. 513 Bhopal – 462 016 Madhya Pradesh	Bhopal	85	22	14	121
16	The Chief General Manager, NABARD, 54, Wellesley Road, Shivaji Nagar Post Box No. 5 Pune - 411 005 Maharashtra	Pune	92	35	16	143
17	The Deputy General Manager, NABARD, Leiren Mansion 2nd Floor, Opp Lamphel Super Market Lamphelpat , Imphal - 795004 Manipur	Imphal	8	3	1	12
18	The Deputy General Manager, NABARD, U PHEIT KHARMIHPEN Building 2nd and 3rd Floor, Plt No. 28(2), Dhankheti, Near Law College Shillong - 793 003 Meghalaya	Shillong	16	4	1	21
19	The General Manager, NABARD, Ramhlun Road (North) Bawngkawn, Aizawl – 796 012 Mizoram	Aizawl	10	4	2	16
20	The Deputy General Manager, NABARD, 4th floor , West Wing Administrative NSCB	Dimapur	11	3	3	17

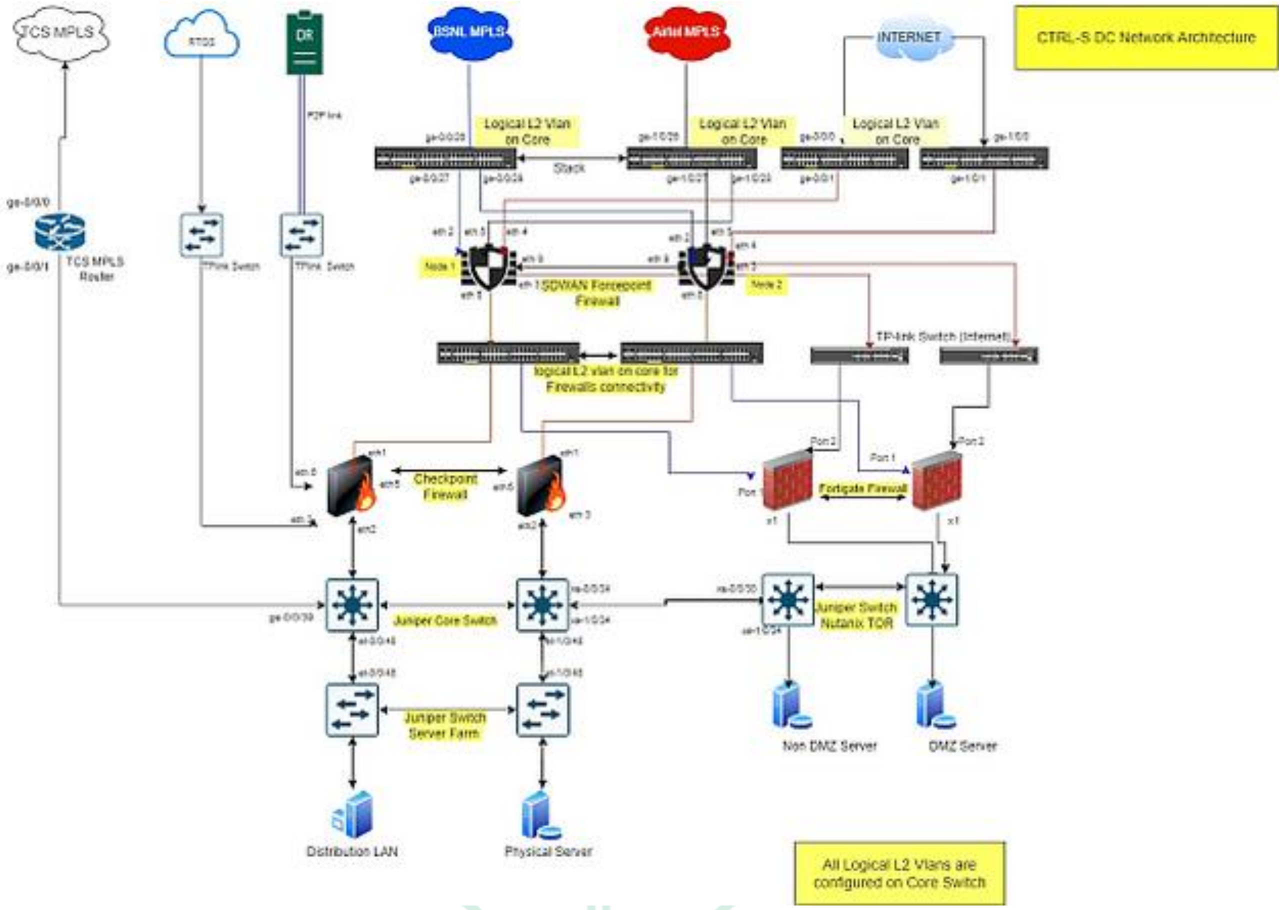
	Building Kher Mahal, Circular Road Dimapur – 797 112 Nagaland					
21	The General Manager, NABARD, 24, Rajendra Place New Delhi - 110 008 Delhi	Delhi	33	10	8	51
22	The Chief General Manager, NABARD, Ankur 2/1, Nayapalli Civic Centre Post Box 179 Bhubaneswar 751 015 Odisha	Bhubaneswar	76	21	12	109
23	The Chief General Manager, NABARD, Plot. No. 3, Sector 34-A Post Box No. 7 Chandigarh – 160 022 Punjab	Chandigarh	60	17	9	86
24	The Chief General Manager, NABARD, 3, Nehru Place, Tonk Road Post Box No. 104 Jaipur – 302 015 Rajasthan	Jaipur	84	17	14	115
25	The Deputy General Manager, NABARD, Om Niwas Church Road Post Box No. 46 Gangtok - 737 101 Sikkim	Gangtok	8	5	3	16
26	The Chief General Manager, NABARD, 48, Mahatma Gandhi Road Post Box No. 6074 Nungambakkam Chennai – 600 034 Tamil Nadu	Chennai	91	23	10	124

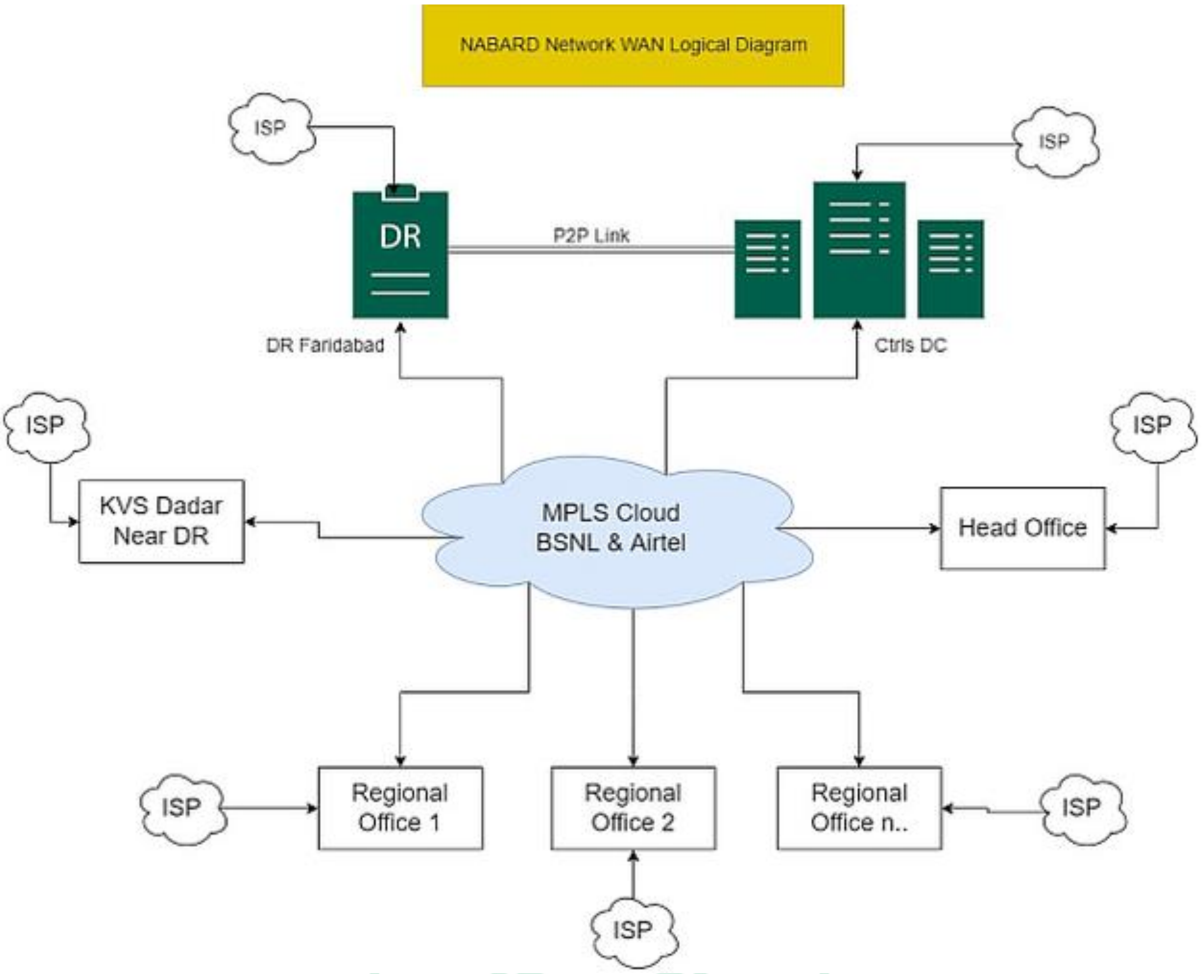
27	The Chief General Manager, NABARD, R.T.C , X Road Musheerabad Hyderabad - 500 020 Andhra Pradesh Telangana	Hyderabad	65	15	21	101
28	The General Manager, NABARD, Shilpa Nigam Bhaban,Ground Floor, Khejur Bagan near Ginger Hotel PO. Kunjaban Agartala - 799006 Tripura	Agartala	10	4	5	19
29	The Chief General Manager, NABARD, 11, Vipin Khand Gomti Nagar Lucknow – 226 010 Uttar Pradesh	Lucknow (RO)	132	26	13	171
30	The Chief General Manager, NABARD, Hotel Sunrise Building 113/2, Rajpur Road Dehradun - 248 001 Uttarakhand	Dehradun	47	10	5	62
31	The Chief General Manager, NABARD, Dp Block Bank Mitra, DP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	Kolkata	67	15	16	98
32	The Director, Bankers Institute of Rural Development, Sector H, LDA Colony, Kanpur Road, Lucknow - 226 012	Lucknow (BIRD)	27	0	0	27
33	The Principal, National Bank Staff college, Sector H, LDA Colony, Kanpur Road, Lucknow - 226 012	Lucknow (NBSC)	22	10	3	35
34	The Principal, Regional Training College, NABARD	Kolkata	11	3	1	15

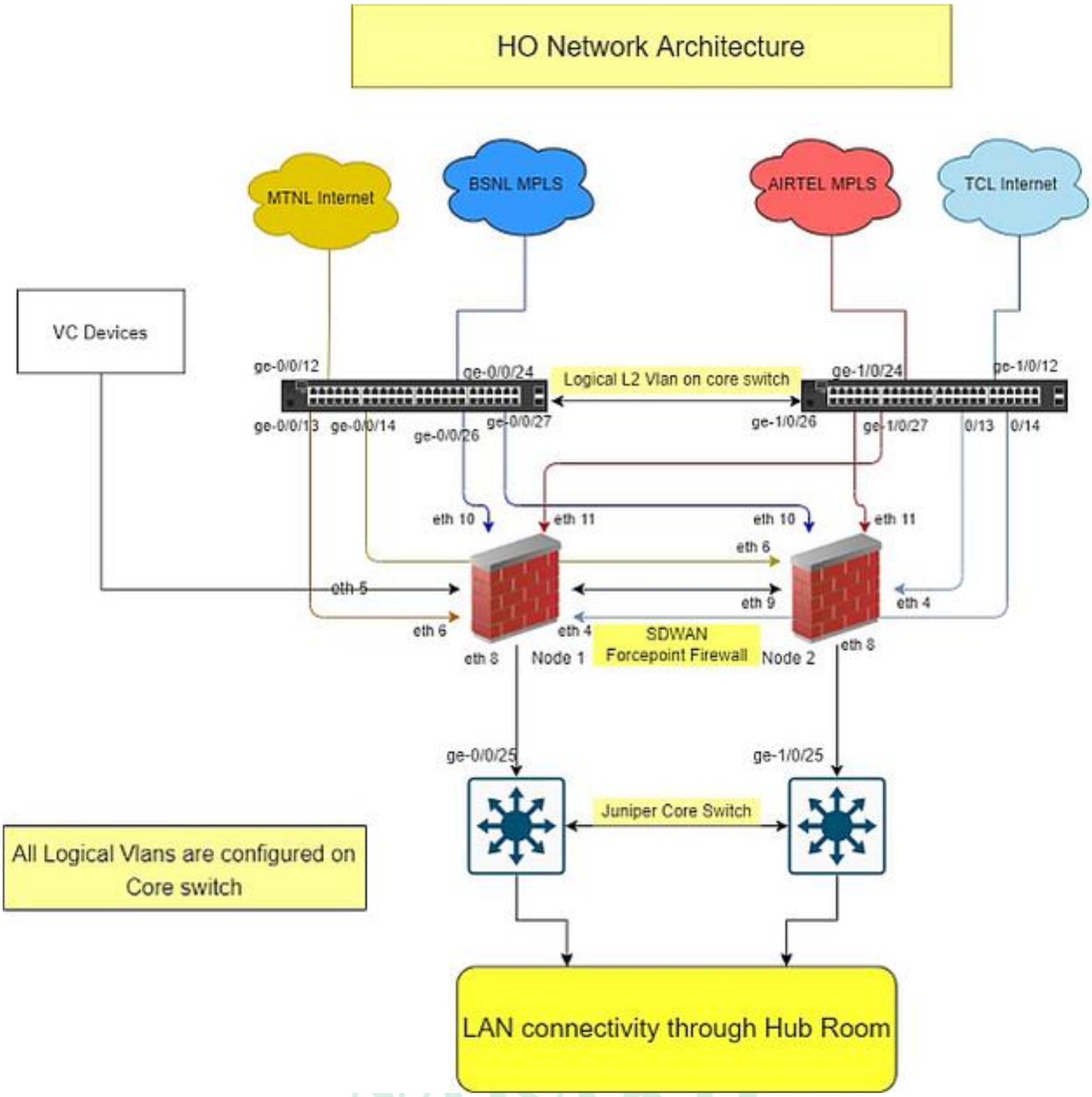
35	The Principal, Regional Training College, NABARD, BIRD Campus, Behind Government Polytechnic for Women, Krishna Nagar Road, Bondel, Mangalore - 575008	Mangalore	13	3	1	17
36	The Chief General Manager, NABARD, Head Office, Bandra-Kurla Complex, Bandra (E), Mumbai 400 051	Mumbai HO	503	192	124	819
37	DR Site of NABARD	Faridabad Datacenter	0	0	0	0

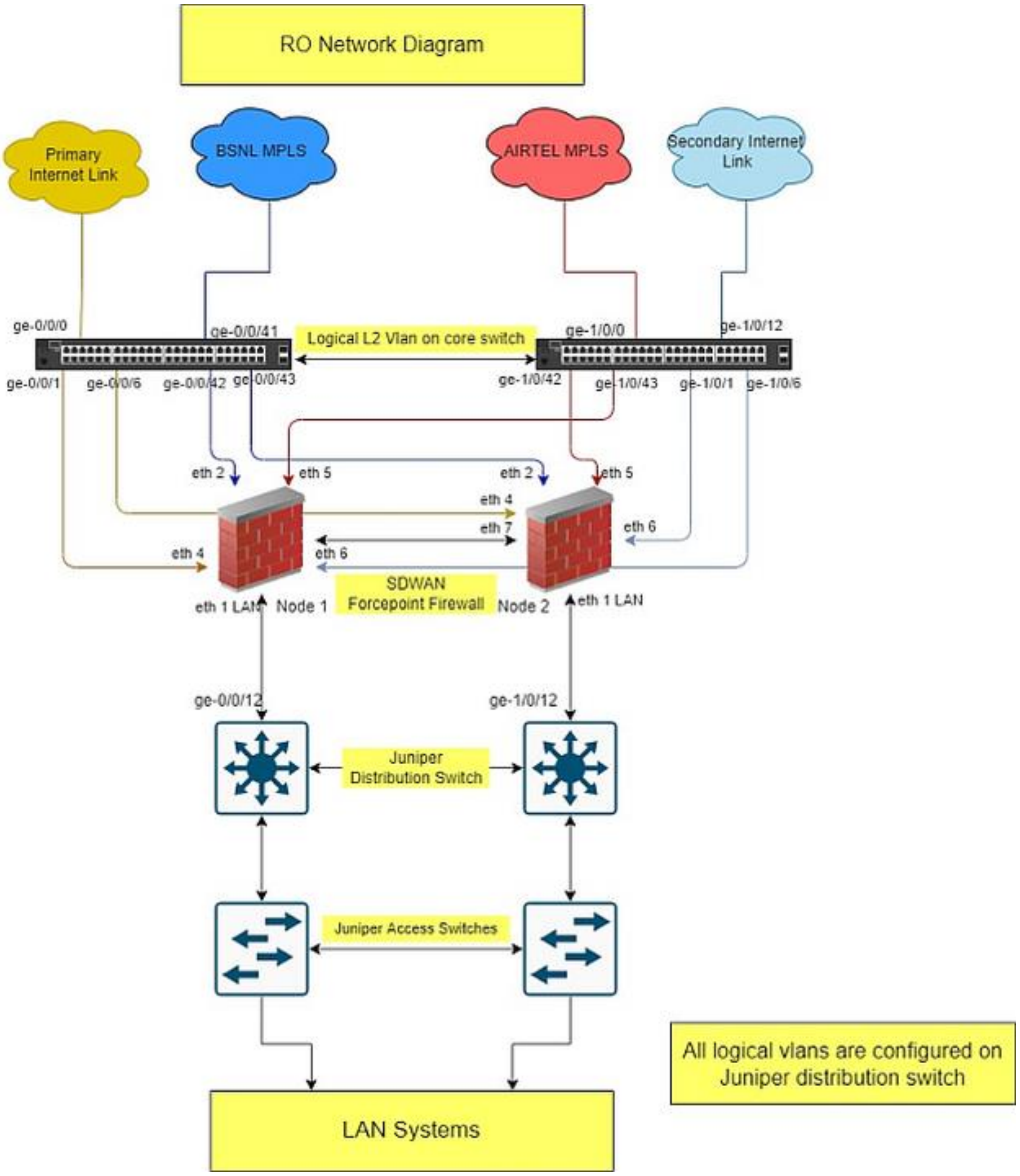
** The complete address will shared with the selected ITSM service provider.

APPENDIX II - Wide Area Network Setup in the Bank




NABARD Network WAN Logical Diagram
ISP
DR
P2P Link
ISP
DR Faridabad
Ctrls DC
ISP
KVS Dadar Near DR
MPLS Cloud BSNL & Airtel
Head Office
ISP
ISP
Regional Office 1
Regional Office 2
Regional Office n..
ISP
ISP


HO Network Architecture
MTNL Internet
BSNL MPLS
AIRTEL MPLS
TCL Internet
VC Devices
ge-0/0/12
ge-0/0/24
Logical L2 Vlan on core switch
ge-1/0/24
ge-1/0/12
ge-0/0/13
ge-0/0/14
ge-0/0/26
ge-0/0/27
ge-1/0/26
ge-1/0/27
0/13
0/14
eth 10
eth 11
eth 10
eth 11
eth 6
eth 5
eth 9
eth 4
eth 6
eth 4
SDWAN
Forcepoint Firewall
eth 8
Node 1
Node 2
eth 8
ge-0/0/25
ge-1/0/25
Juniper Core Switch
All Logical Vlans are configured on Core switch
LAN connectivity through Hub Room


RO Network Diagram
Primary Internet Link
BSNL MPLS
AIRTEL MPLS
Secondary Internet Link
ge-0/0/0
ge-0/0/41
Logical L2 Vlan on core switch
ge-1/0/0
ge-1/0/12
ge-0/0/1
ge-0/0/6
ge-0/0/42
ge-0/0/43
ge-1/0/42
ge-1/0/43
ge-1/0/1
ge-1/0/6
eth 2
eth 5
eth 2
eth 5
eth 4
eth 7
eth 6
eth 4
eth 6
SDWAN Forcepoint Firewall
eth 1 LAN
Node 1
Node 2
eth 1 LAN
ge-0/0/12
ge-1/0/12
Juniper Distribution Switch
Juniper Access Switches
LAN Systems
All logical vlans are configured on Juniper distribution switch

APPENDIX III – Number of Engineers Estimated for Delivery of ITSM

Head Office, Mumbai

Service Components	Minimum Expectations No of engineers Onsite at HO		
	L1	L2	Shared
AMC for Computers and Peripherals +End User Support+ Help/Service desk Management	7	x	x
Network Management	1	1	1(L3)
Firewall + SDWAN + Web Proxy	2	1	x
Antivirus	x	1	x
Windows	1	1	x
Linux	1	x	1(L3)
AIX	x	x	1(L2)
Backup and Storage	x	1	x
DB	1	1	x
Nutanix	x	1	x
SDWAN	1	1	x
Ctrls*	2	x	x
Team Lead	2		
Total	24		

*__Any 2 resources from L1 Network, Antivirus, Windows, Linux__

Locations other than Head Office

S.No.	Location	Number of Onsite End User support engineer
1	Dehradun	2
2	Bhubaneshwar	2
3	Pune	2
4	Bird Kolkata	1
5	Chandigarh (Haryana)	2
6	Delhi	2
7	Bhopal	2
8	Shillong	1
9	Mangalore	2
10	Port Blair	1
11	Jammu	2
12	Andhra Pradesh (HYD)	2
13	Agartala	1
14	Goa	1
15	Imphal	1
16	Ranchi	2
17	Gangtok	1

18	Itanagar	1
19	Aizawl	1
20	Shimla	2
21	Ahmedabad	2
22	Bangalore	2
23	Dimapur	1
24	Chandigarh (Punjab)	2
25	Chennai	2
26	Guwahati	2
27	Telangana (hyd)	2
28	Kolkata	2
29	Thiruvananthapuram	2
30	Patna	2
31	Raipur	2
32	Jaipur	2
33	Lucknow	2
34	Lucknow (Bird)	2
35	Lucknow (NBSC)	3
36	Amravati Cell	1
Total		62

APPENDIX IV – Complete Inventory List of IT Assets / Equipment

A complete IT Assets Hardware Available in the Head Office at Mumbai, all regional offices, Training Establishments is as under:

Total Asset Inventory				
Category	**In AMC**	**In Warranty**	**Out of AMC**	**Grand Total**
Desktop	868	1364	2250	4482
Laptop	226	1035	618	1879
Printer	155	391	1919	2465
Scanner	30	61	289	380
Grand Total	1279	2851	5076	9206

It may be noted that AMC cost will be paid based on actual assets in AMC on pro rata basis cost quoted in commercial bid.

APPENDIX V – Compliance Matrix

Annexure

Compliance Matrix

1. Annual Maintenance Contract (AMC)

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	As and when NABARD acquires new IT asset(s) after the start of this contract, coordination and timely closure of warranty and extended warranty related requirements for all IT assets. If on expiry of essential warranty/extended warranty, NABARD decides to enter into AMC of assets such as Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanner with ITSM service provider, rate for the same will be determined based on the unit rate already decided for the existing item in AMC.			
2.	The type of maintenance will be fully comprehensive on-site including repair /replacement of parts and if not repairable, ITSM will inform NABARD within 7 days. Maintenance Services shall consist of preventive and breakdown maintenance of Desktops, AIOs, laptops, other mobile devices, printers (all type), Scanners.			
3.	A rate card will be part of quote based on SOP for attending to complaints within 48 hours for all district/cluster offices of the bank.			
4.	If 'End of Service Life' (as mutually agreed between NABARD and the Service Provider) of an asset falls in between any quarter during contract period, Service Provider will intimate NABARD at least 90			

<table>
<tr><td></td><td>days in advance for replacement of the same. However, Service provider shall continue to provide AMC and ITSM support for these items till NABARD replaces them with new items.</td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td>At any stage of the contract, NABARD reserves the right to terminate the AMC for any of the item(s), with due prior notice of 30 days to the service provider. Service provider shall raise invoices for all the subsequent quarters after deducting the AMC charges for the items taken out of AMC.</td><td></td><td></td><td></td></tr>
<tr><td>6.</td><td>The current timings for providing AMC services are given below. It is possible that these timings may change in future, but the total working hours will be 9 hours on weekdays.
<table>
<tr><th>Working Day</th><th>Time From</th><th>Time To</th></tr>
<tr><td>Monday to Friday</td><td>9.00 am</td><td>6.00 pm (or as required)</td></tr>
<tr><td>Saturday/Sunday/ Holidays</td><td>As required</td><td>As required*</td></tr>
</table>
*At no additional cost</td><td></td><td></td><td></td></tr>
<tr><td>7.</td><td>The service segment can be split, if need be, into critical and non-critical services for the purpose of round-the clock on-site monitor.</td><td></td><td></td><td></td></tr>
<tr><td>8.</td><td>The complete inventory of all the IT Assets / Equipment which are to be managed and services are given in the <b>Appendix IV</b></td><td></td><td></td><td></td></tr>
<tr><td>9.</td><td>The Service Provider will have to provide support for all computer hardware, software and network related calls as logged by NABARD. Service Provider will</td><td></td><td></td><td></td></tr>
</table>

	be responsible for troubleshooting and resolution of related calls and report them back to Central Helpdesk.			
10.	The Service Provider will undertake to maintain highest service standards as per good industry practice. The Service Provider will arrange for qualified and experienced resident engineers to meet the above-mentioned service levels. For successful implementation and smooth functioning of the operations, personnel with appropriate skills, aptitude and experience would be deputed at NABARD offices. Service Provider shall submit resumes of engineers to be deployed at NABARD. NABARD would have the right to accept / reject the proposed personnel. Also, if any personnel were to quit then handholding would be necessary with suitable replacement with prior notification to NABARD.			
11.	The Service Provider will provide on-site maintenance services. Service Provider should provide PC/Printer/Notebook Computer/Networking equipment in case the problem is not resolved within 4 working hours for the concerned user to carry out his day-to-day work from buffer stock of NABARD. ITSM Service Provider shall provide all essential tools, service kit and testing toolkit needed for maintenance of the computer systems at all locations.			
12.	The ITSM Service Provider shall conduct preventive maintenance as may be necessary from time to time (minimum twice in a year) to ensure that equipment is in efficient running condition to ensure trouble free functioning. **Preventive maintenance Scope** • Physical cleaning using blower. • Bios updates.			

	• OS and antivirus patch updates. • Software updates. • Inventory update • Any other related activity			
13.	The ITSM service Provider shall conduct physical verification of assets minimum once in a year or as need arises.			

2. Desktop Management using the tool

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Taking control of remote desktops using tool.			
2.	Remote Management of Desktops - installation, configuration and troubleshooting of operating system, Anti-virus and all user Applications in the desktops/laptops.			
3.	Remote installation of patches			
4.	Remote Routine maintenance of PCs (e.g., cleaning up file system debris, defragmenting drives, running malware scans, etc.)			
5.	Taking back-up while configuring new systems.			
6.	Guide and direct users to relevant desk/department/individuals in case support required is not under scope of deliverables by the ITSM Service Provider and carrying out related activities.			
7.	Use latest technology for bulk installation for multiple machine.			
8.	Special Note: Desktop management services are required to be provided for IT			

	equipment (i.e. PC/AIO, Printer, Laptop, Scanner, Internet etc.) at the residences of senior executives (CGM/OIC and above) at all locations.			
9.	Taking back-up while configuring new systems.			
10.	Guide and direct users to relevant desk/department/individuals in case support required is not under scope of deliverables by the ITSM Service Provider and carrying out related activities.			
11.	Use latest technology for bulk installation for multiple machine.			
12.	Special Note: Desktop management services are required to be provided for IT equipment (i.e. PC/AIO, Printer, Laptop, Scanner, Internet etc.) at the residences of senior executives (CGM/OIC and above) at all locations.			
13.	Guide and direct users to relevant desk/department/individuals in case support required is not under scope of deliverables by the ITSM Service Provider and carrying out related activities.			
14.	Use latest technology for bulk installation for multiple machine.			

3. Inventory Management using tool

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Capable of installation, configuration and using the			

	tool (import of existing data).			
2.	Should maintain the Catalog of software and hardware from all major OEMs/Principals and should update the signature for the same on periodic basis. The update periodicity should be as per industry norms.			
3.	Managing Configuration Management data base (CMDB).			
4.	Initially, complete inventory of all IT assets in the Bank has to be taken up independently with relevant tools and the same has to be shared with the Bank and later on periodicity as decided by bank.			
5.	Dashboard to identify the addition and deletion of IT assets in the Bank for custom period.			
6.	Capable of Configuration item (CI) identification, planning and controlling configuration changes			
7.	Capable of configuration change report generation			
8.	The service provider will do the lifecycle management of the licenses including initiation of procurement request, after purchase, allocation, de-allocation, license renewal alert, license pool management.			
9.	Software Licenses Tracking & Management - This includes number of licenses for particular software, which NABARD has purchased, how many have been deployed, what is the entitlement etc.			
10.	Should support management of multiple licensing models based on User, Machine, IP, Core etc.			

11.	And any other related activities.			

4. Patch Management using the tool

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	The ITSM service should include a patch management solution that offers all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating systems.			
2.	All critical application/software should also be patched as soon as patch/upgrade is available.			
3.	Assist, Develop, Manage and Monitor suitable Policies, Procedures and deployment strategy for Patch Management.			
4.	Maintain an up-to date plan for deploying and managing patch management.			
5.	Install and test patches and updates in Test environment provided by NABARD and after approval roll-out in the client computers			
6.	A practical and up-to date roll back plan has to be adopted in case of failures.			
7.	Raise Change Management for deployment of patches or updates.			
8.	Schedule shutdown of production system and inform users before applying patches, updates to Servers.			

9.	Implement patches as per approved deployment strategy.			
10.	Follow up and co-ordinate with OEM/ 3rd party support ITSM Service Providers for patch deployment on all devices.			
11.	Build a suitable backup and disaster recovery procedure for maintaining 100% availability of the Patch Management Server and resources.			
12.	Report on installed and missing patches			
13.	Removal of Software and service packs in case of need and roll back of patches and service packs in case of need			
14.	Capability to identify the devices where patches are applied but not yet activated (pending restart)			
15.	A quarantine area has to be maintained for isolating the devices that are not patched up/updated with requisite updates.			
16.	Able to communicate effectively at all levels of the organization, and with ITSM Service Providers, in written and oral format.			
17.	Maintain smooth operation of multi-user computer systems, including coordination with network, software, and system engineers, PC desktop technicians, project managers, end users, and customer and IT management.			
18.	Interact, meet, discuss, and troubleshoot issues with ITSM Service Providers; evaluate ITSM Service Provider products, services, and suggestions.			
19.	Maintain security audit information in tracker sheet			

	for all patching related activities.			
20	The tracker to be shared with DIT on weekly basis for review.			
21.	Solution should support system architectures.			

5. Domain Services Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Existing Domain Server and User Admin have to be managed effectively with the help of suitable tools.			
2.	The service should include plan, design and set up and upgrade of additional controllers/forest during the contractual period.			
3.	Should co-ordinate, guide and assist in integrating any other systems for SSO /2FA and also digital certificate.			
4.	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.			
5.	Administrative support for user registration, creating and maintaining user profiles, granting user			
6.	Periodic reviews of domain level rights and privileges			
7.	Periodic AD (Active Directory) data updation and data			

	interlinking with HRMS for auto updation.			
8.	AD integration with other applications			
9.	Any other related/similar activities.			
10.	Existing Domain Server and User Admin have to be managed effectively with the help of suitable tools.			
11.	The service should include plan, design and set up and upgrade of additional controllers/forest during the contractual period.			
12.	Should co-ordinate, guide and assist in integrating any other systems for SSO /2FA and also digital certificate.			
13.	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length. Password complexity, password expiry, account lockout policy, certificate policies. IPSEC policies etc.			
14.	Administrative support for user registration, creating and maintaining user profiles, granting user			
15.	Periodic reviews of domain level rights and privileges			
16.	Periodic AD (Active Directory) data updation and data interlinking with HRMS for auto updation.			
17.	AD integration with other applications			

6. File Services Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance

1.	Storage management: This console allows administrators to manage shared folders and allows users to access shared folders over the network.			
2.	Distributed File System (DFS): Provides tools and services for DFS Namespaces and Replication services.			
3.	DFS Namespaces: Allows user to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears as a single shared folder with a series of subfolders.			
4.	Replication: Allows to synchronize files/folders on multiple servers across the network.			
5.	File Search: Fast file search capabilities			
6.	Indexing service: Allows indexing of files and folders for faster searching.			
7.	The access to files should be based on User Rights controlled by Domain Services.			
8.	Selective Syncing of data in fileserver with cloud.			
9.	The ITSM Service Provider should be capable of installation, configuration, and management of the above stated file server.			
10.	Replication of the files/folders and capable of handling the File Services Management functionality.			

7. Storage Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
Incident Management				
1.	Development of storage management policy,			

	configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.			
2.	Configuration of SAN whenever a new application is hosted on the SDC. This shall Include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc			
3.	Monitoring service availability, resource usage			
4.	Troubleshooting system alerts with knowledge base			
5.	Network reachability			
6.	Administer SAN storage arrays and SAN fabrics and Participate in SAN on-call rotation			
7.	Providing timely compliance to the audit observations related to storage infrastructure as observed during various internal/ external audits			
8.	Preparation/Revision of Standard Operating Procedure (SOP) document for the Storage Administration.			
Problem Management				
9.	Closure of incidents effectively.			
10.	Liaise with service providers for escalation and Root cause analysis			
11.	Preparation of Preventive Maintenance calendar and configuring replication.			
12.	SAN / NAS access control review.			
Performance & Audit Management				
13.	Monthly / Fortnightly incident analysis.			
14.	Audit of administrator accounts.			

15.	Preparation of capacity planning report.			
Backup Management (All Servers at DC and DR)				
16.	Performing backup operations for the servers as per the defined backup strategy.			
17.	Ensuring proper storage and handling of media to prevent data loss.			
18.	Conducting restoration drills with sample backed-up data on a quarterly basis to confirm data integrity.			
19.	Maintaining log sheets of backups taken.			
20	Implementing best practices on backup.			
21.	Installation, re-installation, upgrade and patch deployment of the Arcserve, HPDP, etc. in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.			
22.	Generation and publishing of backup reports periodically			
23.	Coordinate with the backup tape movement service provider/ courier agency and the identified nodal officer(s) for sending/ receiving tapes.			
24.	Coordination for maintaining inventory of off-site tapes at respective locations i.e., DC, DR, Head Office etc.			
25.	Tape/ LTO library management – loading and unloading tapes, etc at DC & DR.			
26.	Forecasting tape requirements and giving timely indent to concerned team for timely procurement of the new tapes/storage			
27.	Reporting of failed backups with critical alerts and ensuring that those are restarted and completed			

	successfully within the backup cycle			
28	Update/ Maintain Standard Operating Procedure (SOP) documents			
29.	Regular review of backup process and assist team to manage capacity planning.			
30	Weekly movement of tapes between DC and Head Office, Mumbai, Delhi RO and DR site (Preferably on Friday)			
31.	Insertion of tapes in tape library at DC & DR site			
32.	Ejection of tapes from tape library at DC & DR site.			

8. Data Center and Server Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Regularly monitor and log the state of environmental conditions and power conditions in the Datacenter.			
2.	Service support at DR is required as and when required.			
3.	Periodic review arrangements at Data Center(DC&DR) in terms of cooling, power, positioning of racks &other hardware etc. on an annual basis. The SP shall be required to do first such assessment and submit a report thereon within a period of 2 months from the date signing of contract.			
4.	Coordinate with NABARD and third-party Service Providers to resolve any problems and issues related to the Datacenter & DR Site environment conditions. Power, air-conditioning, UPS, LAN, Servers, racks, fire, water seepage, dust			

	cleanliness, implementing any changes, layout of infrastructure within the Datacenter & DR Site etc.			
5.	Suggest/Assist NABARD on best practices of the industry which may be required to be implemented in Data Center.			
6.	Patch management, upgrades to the systems.\			
7.	Ensure compliance of NABARD IT Security policies and compliance pertaining to Physical Security equipment in the DC.			
8.	Maintain high server availability through active performance monitoring and low impact, on- demand remote management services for devices present at DC&DR.			
9.	Installation, Updation configuring, hardening, trouble shooting of system (Hardware, Firmware and software) across all locations of NABARD			
10.	Mounting and Unmounting of all hardware components and Cabling, labling, tagging.			
11.	In case of repetitive hardware failure (three times in a period of three months) during warranty and AMC period, ITSM should coordinate to ensure that they are replaced by equivalent new equipment by OEM/Vendor as per SLA between NABARD and OEM/vendor.			
12.	Capacity planning and life cycle management of servers and other hardware and IT systems.			
13.	Inventory management of all the hardware devices including spare materials and periodical updation and review of the same			

14.	Regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.			
15.	All firewall, critical servers logs to be maintained for a period defined by NABARD.			
16.	Management of load balancers			
Manage Nutanix Virtualized environment and other HCI virtualized environment. The Nutanix (Virtualization) skill set requirements				
17.	Knowledge and administration of industry leading virtualization software / technologies.			
18.	Knowledge of Nutanix virtualization, VM replication, FLOW, XPLAY, prism central, etc.			
19.	Design and develop service virtualization framework.			
20	Configure, deploy, monitor and support Nutanix nodes and clusters.			
21.	Define best practices, processes for service virtualization.			
22.	Maintain and configure Service Virtualization tool.			
23.	Troubleshoot the issues.			
24.	System installation and maintenance of Windows, AIX and Linux systems.			
25.	Windows, Linux, AIX, Arcserve, HPDP and Nutanix administration.			
26.	Knowledge of data center operations.			
27.	Administration of DNS (IPAM), SMTP, FTP, SSH, LDAP, and NFS services.			
28	Patch management, upgrades to critical systems.			
29.	SAN/NAS storage systems knowledge.			
30	Hardware, software and network troubleshooting.			

31.	Understanding of new business initiatives and the implementation of technologies to facilitate them.			
32.	Manage systems to achieve 24x7 availability.			
33.	Work closely with the storage, network and development groups to ensure business continuity.			
34.	Conduct trainings, mentor and coach teams on Service Virtualization			
35.	Valid Nutanix NCP-MCI-5 certification or higher.			
36.	Administering/monitoring Nutanix PRISM Console along with Nutanix nodes, clusters, hosted VMs in DC and DR. Further, the SP shall also monitor, upgrade and update Acropolis OS, AHV Hypervisor etc. Work will involve regular creation of VMs, cloning and monitoring performance of each VM. This shall require conducting regular health checkups and submit regular reports on overprovisioned VMs in terms of RAM, memory, cores etc. for the VM and cluster. Perform capacity planning from time to time.			
37.	Regular co-ordination and advisories related to the conduct of DR Drill which take place every quarter.			
38	To act as a trusted advisor to customer IT Teams, providing guidance as well as suggesting Nutanix and other VMware best practices.			
39.	Windows, Linux, AIX, Arcserve, HPDP and Nutanix administration.			
40	Knowledge of data center operations.			

41.	Administration of DNS (IPAM), SMTP, FTP, SSH, LDAP, and NFS services.			
42.	Patch management, upgrades to critical systems.			
43.	SAN/NAS storage systems knowledge.			
44.	Hardware, software and network troubleshooting.			
45.	Understanding of new business initiatives and the implementation of technologies to facilitate them.			
46.	Manage systems to achieve 24x7 availability.			
47.	Work closely with the storage, network and development groups to ensure business continuity.			
48	Conduct trainings, mentor and coach teams on Service Virtualization			
49.	Valid Nutanix NCP-MCI-5 certification or higher.			
50.	Administering/monitoring Nutanix PRISM Console along with Nutanix nodes, clusters, hosted VMs in DC and DR. Further, the SP shall also monitor, upgrade and update Acropolis OS, AHV Hypervisor etc. Work will involve regular creation of VMs, cloning and monitoring performance of each VM. This shall require conducting regular health checkups and submit regular reports on overprovisioned VMs in terms of RAM, memory, cores etc. for the VM and cluster. Perform capacity planning from time to time.			
51.	Regular co-ordination and advisories related to the conduct of DR Drill which take place every quarter.			
52.	To act as a trusted advisor to customer IT Teams, providing			

	guidance as well as suggesting Nutanix and other VMware best practices.			
JBoss Administration				
53.	Support for CLMAS Upgrade for NABARD and its subsidiaries and RADP Platform			
54.	JBoss Installation and JDK configuration			
55.	JBoss Hardening and Upgrade			
56.	.ear, .jar, .war file Deployment			
57.	.jsp file attachment in tmp folder			
58.	App to Database connectivity configuration			
59.	Java Heap size changes			
60	Port configuration (8080,18080, http and https)			
61.	Process kill JBoss			
62.	JBoss Service start / stop			
63.	Logs monitoring			
64.	New instance creation			
65.	Configuration file changes			
66.	SSL certificate installation			
67.	Daily Health checkup of JBoss Application Server			

9. Network Management Services

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
Monitoring:				
1.	Bandwidth utilization			
2.	QoS and traffic shaping requirements/SDWAN management			
3.	Link latency			
4.	Uptime			
5.	Port utilization and growth			
6.	Marry port and patch panel utilization for audits			

7.	Audit and advice on rack utilization and growth			
8.	Inform the County of growth requirements for cabling such as network drops or fiber backbone Monitoring of Traffic Pattern over WAN			
9.	Follow up with Regional Offices for connectivity related issues			
10.	Monitoring and troubleshooting of L2 /L3 switches.			
11.	Monitoring Jitter, Latency, Availability, Bandwidth usage			
12.	Managing existing Firewalls, UTM, and VPN Services.			
13.	SDWAN monitoring, management and troubleshooting.			
14.	Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.			
15.	Managing NAC setup.			
16.	Managing Wi-Fi setup.			
17.	SFMS support			
Vendor Management				
18.	Enforcing SLAs with external networking ITSM Service Providers			
19.	Opening and managing support cases with external networking ITSM Service Providers/ISPs for various issues such as offline connections and SLA violations			
20.	Maintaining escalation matrix and ensuring the creation escalation matrix wherever required.			

21.	BGP etc and other NOC related coordination with ISP			
22.	OEM/SI related coordination for hardware issues.			
23.	Coordinate with these ITSM Service Providers for support services.			
24.	Maintain good relations with them on behalf of NABARD.			
25.	Logging calls, coordination and follow-up with ITSM Service Providers.			
26.	Escalation of calls to the higher levels at ITSM Service Provider side in case of requirement.			
27.	AMC/ Warranty/ Support Tracking			
28.	Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the ITSM Service Provider will be made separately by NABARD)			
29.	Management of assets sent for repair.			
30.	Maintain database of the various ITSM Service Providers with details like contact person. Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with ITSM Service Providers, Coordinate and			
31.	Analyze the performance of the ITSM Service Providers periodically (Quarterly basis or as specified).			

32.	Keep NABARD updated on the services and performance of these third-party ITSM Service Providers.			
33.	When a new solution software is introduced, training to users to absorb and leverages the technology for business should be invariably arranged.			
Administration				
34.	Managing routers, switches, firewalls, load balancers, wireless access points, and any other networking equipment			
35.	Assigning, allocating, and auditing network ports			
36.	Assigning and reassigning VLANs			
37.	Administering QoS policies as needed			
38.	Administering 802.1X authentication configurations where applicable			
39.	Firmware, application, controller, and operating system patching and maintenance			
40.	Maintain, audit, and extend the given IP schema and routing architecture			
41.	IPv4 with the intention to include IPv6 in the future			
42.	Maintain, audit, and extend multicast support throughout the network where applicable			
43.	Any other work assigned from time to time.			

44.	IS audit related information should be provided by the ITSM Service Provider.			
45.	Providing GUI based interfaces to readily check MPLS links status and utilization, health status of devices, Application based traffic (QOS) across all the locations ROs/HO			
	Lifecycle Management			
46.	Inform the bank of bandwidth requirement/infrastructure upgrade and upgradation on a quarterly basis.			
47.	Participate in the identification and purchase of additional or replacement equipment			
	New Project inclusion:			
48.	In case bank is in process of implementing a new project. The requisite change request for successful implementation and management of the project should be submitted by ITSM Service Provider on request			
	FMS services for Network at HO/DC			
	Monitoring			
49.	Monitoring of the main/backup Links and reporting\			
50.	Monitoring of Bandwidth utilization, latency, packet loss etc.			
51.	Managing NAC setup.			
52.	Managing Wi-Fi setup.			
53.	Monitoring of Traffic Pattern over WAF			

54.	Follow up with Regional Offices for connectivity related issues			
55.	Monitoring and troubleshooting of L2 /L3 switches.			
56.	Monitoring Jitter, Latency, Availability, Bandwidth usage			
57.	Managing existing Firewalls, UTM, and VPN Services.			
58.	SDWAN monitoring, management and troubleshooting.			
59.	Managing and troubleshooting of ILL, MPLS, RTGS(IFTAS) links.			
60.	Incident Management			
61.	Call logging and co-ordination with MPLS VPN service provider for restoration of link			
62.	Co-ordination with MPLS VPN service provider for ensuring backup Inks are made operational in the event of failure of primary and secondary links			
63.	Follow up with Service Provider to get detailed RFOs/RCA.			
64.	Prepare the Link wise outages and calculate the SLA Report to enable processing of the Service Provider Invoices			
65.	Prepare the Detailed payment note for due processing depending on SLAs.			
66.	Configuration Management			
67.	Configuration of L2 switches for administration and L3 Switches for VLAN			

	creation / hardening etc.			
68.	Installation & Upgrade of switches as and when provided by the OEM/SI.			
69.	Changing configuration based on NABARD requirement and follow-up with MPLS VPN service provider for application of same on all routers.			
70.	Maintaining / Updating the WAN diagram at all locations/offices in co-ordination with NABARD IT team and Local Service Provider			
71.	Maintaining complete inventory of network hardware along with interfaces. IP address, Device OS version etc.			
72.	Reporting			
73.	Maintenance of daily/Weekly and monthly uptime report.			
74.	Collection of daily / weekly and monthly uptime/downtime report from MPLS VPN service provider.			
75.	Verification of daily report with the fault ticket generated by the MPLS VPN Service provider.			
76.	Cross verification of daily report with weekly and monthly report and calculation of uptime / downtime.			
77.	Co-ordination with MPLS Service provider for the replacement/up keep			
78.	Maintenance of defective Networking Hardware/Software			

	(Like Routers. Modems. Switches etc.) and escalation, if necessary.			
79.	Advisory Services			
80.	Advisory services for revamping networks and introducing new network devices and services are also needed.			
81.	Periodic review mechanism should also be introduced for service improvements in this work area.			
	a. **Onsite Support Engineer's Role for Network Animator tool (But not limited to this),**			
82.	The engineer will perform following L1/L2 tasks in NMS solution with regards to the tools implemented at bank.			
83.	Perform daily tools health check based on checklist (services, processes, log file for any errors, application disk.			
84.	Perform all L1 level troubleshooting (Tool Management System Level) and assist Bank's Network Support team for troubleshooting.			
85.	Perform MACD (Move/Add/Change/Delete) activity such as adding/removing N/W devices, Servers from,			
86.	Perform Tasks like adding/modifying assignment group members, categories.,			
87.	Perform L1 level troubleshooting and follow L2 escalation matrix for non-resolved incidents.,			
88.	Coordinating for for L2 troubleshooting.,			

89.	Act as coordinator and provide assistance to OEM's remote support teams for troubleshooting/resolving the product,			
90.	Ensure all Service Requests, Incident and changes are logged and tracked till closure.,			
91.	Generating out of box reports as and when required by Bank.			
92.	Analyze network bandwidth report and device utilization to advice NOC team for Bandwidth up-gradation etc.			
93.	Daily MIS reporting of all the critical links.			
94.	Log the call with the OEM for critical tools issues,			
Onsite Support Engineer's Role for NCCM tool (But not limited to this)				
95.	Any configuration changes requested by bank forDC/DR or branch devices.			
96.	Take care of configuration change and roll back as per bank person request.,			
97.	Do the solution fail over testing on critical devices b/w NLS and DR on weekly basis.,			
98.	Take back up for all network and security devices on daily basis.,			
99.	Creating any new configuration/ configuration template/job/tasks etc as and,			
100.	DC/DR/Branch devices hardening configuration changes as per banks network,			

101.	Syncing of DC& DR devices on weekly basis.,			
102.	Monitor the solution intimate banks on any compliance breach & rectify based on bank team request as and when required.,			
103.	Share compliance report on daily basis.,			
104.	Inform banks team in case of any alert /error observed in any device configuration and act according to,			
105.	Failover testing of critical devices on weekly basis as per bank team's request.,			
106.	Ensure that all backups are happening correctly and need to maintain and submit the checklist on,			
107.	Prepare and submit day to day activity report on daily basis.,			
108.	Periodic discovery of all all the network devices & share the list of noncompliance devices and do the required changes to make it compliant only after bank's team permission.,			
	SDWAN Forcepoint SMC			
109.	Management of the architecture – documentation of present architecture, BGP peering management with ISP.			
110.	IP Sec tunneling for various sites and traffic management on the tunnels			
111.	Routing on various devices at ROs/HO			

112.	QOS as per Banks requirement			
113.	Configuration of Any other feature available on SDWAN as required by bank			
Wifi controller				
114.	Definition of levels according to network security			
115.	Management of Guest access			
116.	Management of access privileges.			
Support services for CCIL, RTGS/NEFT applications and payment infrastructure management:				
117.	Onsite support for issue-resolution on all working days and as per emergency requirement beyond working days and holidays.			
118.	Remote support Telephonic / Network			
119.	Preventive Maintenance and System Health Checks			
120.	D.R. Drill assistance			
121.	Upgrade / Version Management			
122.	Re-installation / Re-location of Systems and Applications			
123.	License Management (Track and coordinate for validity)			
124.	CCIL Systems Help Desk Support			
125.	Single point of contact for			
126.	Regulatory Authorities (RBI, IDRBT, CCIL)			
127.	Applications vendor			
128.	Principals (IBM, Microsoft, Cisco etc.)			
129.	Service Window			

9. IT Security Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
A suitable Syslog Server has to be incorporated with the following capabilities:				
1.	Collects logs from heterogeneous sources.			
2.	Decipher any log data regardless of source and log format			
3.	Rule-based event correlation for proactive threat management			
4.	Pinpoints breach attempts, insider threats, policy violations, and more, without any manual intervention			
5.	Generate pre-defined compliance reports for event logs and syslogs to meet various standard compliances like PCI DSS and etc.			
6.	Facilitate to create custom reports for new compliance to help comply with growing new regulatory acts demanding compliance in future.			
7.	Generate an alert in case of failure of log collection in regard with any log sources.			
Incident Management Services				
8.	Perform continuous Monitoring on WAF and Web Proxy Consoles.			
9.	Prevention duties include system monitoring, assessment, testing, and analysis designed to identify and correct potential security breaches.			
10.	Protect and improve organizational security by preventing, averting, and mitigating security threats.			
11.	Perform following steps: Incident logging, Incident categorization, Incident prioritization., Incident assignment., Task creation and			

	management., SLA management and escalation., Incident resolution.			
12.	Have collaboration with ITSM Security Team, ITSM Patch ITSM ITSM Service Provider and ITSM Network team to perform incident Analysis.			
13.	Analyze daily reports (AV reports network devices reports, IPS, etc.).			
14.	Creation and Maintaining of Tracker for incidents.			
15.	Perform RCA for Cyber security incidents (email phishing, Antivirus infections, repeated logout, etc.).			
16.	Preparing documentation for each incident analyzed.			
17.	Providing support for application-level settings at WAF.			
18.	Providing support for blocking /allowing any website at web proxy solution. Need to raise a ticket/case with OEM to resolve the website issue if any.			
	Firewall Security and Configuration Management			
19.	Centrally collect, analyze and archive logs from all security devices			
20.	Automate compliance audits with reports for regulatory mandates such as PCI-DSS, ISO 27001, etc.			
21.	Perform firewall rule base review and device configuration analysis and Generate reports on quarterly basis.			
22.	Get real time alert on ‘who’ made ‘what’ changes, ‘when’ and ‘why’ to firewall configuration			
23.	Change management reports to get a complete trail of all the changes done to firewall configuration			
24.	Monitoring Internet usage (overuse and misuse) of employees			

25.	Monitoring outgoing traffic through the proxy, obtain details on user generating traffic, website access and bandwidth consumed			
26.	Real-time notification when a user tries to access restricted sites			
27.	Network traffic monitoring to get instant notifications upon sudden spike in bandwidth			
28.	Analysis of user or network activity consuming high bandwidth with interface-wise bandwidth usage reports			
29.	Getting detailed information on all possible network attacks and security breaches in organization’s network			
30.	Knowing which viruses, malware, BOTs, APT, etc are active on the network, the hosts that are affected and more; Searching logs and report generation based on search results			
31.	Identifying highly used firewall rules which can be optimized to enhance network security			
32.	Identifying unused rules and/or modifying/removing them to improve firewall performance (to comply with all IS policy requirements of GoI/CISO)			
33.	All important GoI and Industry websites needs to be monitored regularly for various policy updates and with suitable approval from IT team of the Bank. All necessary and suitable policies should be applied by the ITSM Service Provider			
34.	Security Information and Event Management (SIEM)			
35.	The monitoring of endpoints, vulnerability information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS) and detection (IDS) systems			

36.	All important GoI and Industry websites needs to be monitored regularly for various policy updates and with suitable approval from IT team of the Bank. All necessary and suitable policies should be applied by the ITSM Service Provider			
37.	Security Information and Event Management (SIEM)			
38.	The monitoring of endpoints, vulnerability information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS) and detection (IDS) systems			
Privileged Password Management				
39.	Storage and organization of all privileged identities in a centralized vault			
40.	Secure sharing of administrative passwords with the members of the team on need basis			
41.	Self-resetting of passwords			
42.	Controlling access to IT resources based on roles and job responsibilities			
43.	Auditing of all privileged accesses and complete recording of all actions			
Network Behaviour Anomaly Detection				
44.	Monitoring network security in real time			
45.	Monitoring internal and external threats			
46.	Classifying threats into various categories (e.g., DDoS, Scan/probe, Suspect, etc)			
47.	Carrying out detailed forensic investigation			
48.	Sending alert notification via Email or SMS			
Active Directory Management and Reporting				
49.	Automatic routine AD management and reporting activities for AD administrators			

50.	Facilitates creation, management, and deletion of AD objects in bulk.			
AD Self-Service Password Management				
51.	Allow users to reset/change their passwords and unlock their AD accounts, without ITSM team intervention through web based portal using SMS and authenticator			
52.	Remind users automatically about soon-to-expire passwords by email and SMS			
53.	Allow users to update their profile details, like contact details in Active Directory through web based portal.			
54.	Allow users to reset/change their passwords and unlock their AD accounts, without IT intervention through web based portal using SMS and authenticator			
Network Configuration Management				
55.	Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI			
56.	Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes			
57.	Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.			
58.	Automating all repetitive, time-consuming configuration management tasks. Applying configuration changes in bulk to multiple devices.			
59.	Recording sessions: Getting complete record of who, what and when of configuration			

	changes. Recording actions, archiving.			
60.	Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI			
61.	Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes			
62.	Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.			
63.	Automating all repetitive, time-consuming configuration management tasks. Applying configuration changes in bulk to multiple devices.			
64.	Recording sessions: Getting complete record of who, what and when of configuration changes. Recording actions, archiving.			
Active Directory Backup and Recovery				
65.	Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI			
66.	Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes			
67.	Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.			
68.	Automating all repetitive, time-consuming configuration management tasks. Applying			

	configuration changes in bulk to multiple devices.			
69.	Recording sessions: Getting complete record of who, what and when of configuration changes. Recording actions, archiving.			
70.	Automated incremental backup of Active Directory Objects			
71.	Change tracking to undo changes			
72.	Detailed version management to each attribute change			
73.	Provision to roll back Active Directory to an earlier state			
74.	Managing configurations: Backup device configurations, maintain history, compare versions and upload changes - all from a centralized GUI			
75.	Taking control of changes: Monitoring configuration changes, get instant notifications, and preventing unauthorized changes			
76.	Ensuring compliance: Define standard practices and policies and automatically check device configurations for compliance. Generate reports on compliance status.			
77.	Automating all repetitive, time-consuming configuration management tasks. Applying configuration changes in bulk to multiple devices.			
78.	Recording sessions: Getting complete record of who, what and when of configuration changes. Recording actions, archiving.			
79.	Automated incremental backup of Active Directory Objects			
80.	Change tracking to undo changes			
81.	Detailed version management to each attribute change			
82.	Provision to roll back Active Directory to an earlier state			
Other Services				
83.	Periodic reviews of domain level rights and privileges			

84.	Modifying access permissions and adding new access permissions of security policies on existing firewall.			
85.	Up-gradation of the firewall and IPS devices.			
86.	Signature update for IPS device.			
87.	Configuration backups for all security devices			
88.	Syslog server configuration & management including review of logs.			
89.	Managing / monitoring the IDS/IPS tool and policies as per guidelines of NABARD.			
90.	Modifying the policy for IDS/IPS/Firewall based on observed trends / security lapses.			
91.	Changing network address translation rules of existing security policies on the firewall.			
92.	Adding new network address translation rules on security policies on existing firewall.			
93.	Diagnosis and troubleshooting of the problem faced on firewall and faced by the IDS/IPS.			
94.	Managing / monitoring the IDS/IPS tool and policies			
95.	Periodic / Critical reporting to NABARD officials based on Firewall / IDS / IPS activities			
96.	Managing configuration and security of Demilitarized Zone (DMZ)			
97.	Alert / advise NABARD about any possible attack / hacking of services, unauthorized access / attempt by Mental or external persons etc.			
98.	Resolution and restoration of services in case of any possible attack and necessary disaster management			
99.	Shutdown of critical services to prevent attack (internal or external)			
100.	Advise to improving network/Data Center security to protect NABARD's data /			

	information from both internal and external persons/attack.			
101.	Resolution and restoration of services in case of any possible attack and necessary disaster management.			
102.	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as			
103.	And other related essential activities to ensure that the functionalities of IT Security.			
104.	Periodic reviews of domain level rights and privileges			
105.	Modifying access permissions and adding new access permissions of security policies on existing firewall.			
106.	Up-gradation of the firewall and IPS devices.			
107.	Signature update for IPS device.			
108.	Configuration backups for all security devices			
109.	Syslog server configuration & management including review of logs.			
110.	Managing / monitoring the IDS/IPS tool and policies as per guidelines of NABARD.			
111.	Modifying the policy for IDS/IPS/Firewall based on observed trends / security lapses.			
112.	Changing network address translation rules of existing security policies on the firewall.			
113.	Adding new network address translation rules on security policies on existing firewall.			
114.	Diagnosis and troubleshooting of the problem faced on firewall and faced by the IDS/IPS.			
115.	Managing / monitoring the IDS/IPS tool and policies			
116.	Periodic / Critical reporting to NABARD officials based on Firewall / IDS / IPS activities			

117.	Managing configuration and security of Demilitarized Zone (DMZ)			
118.	Alert / advise NABARD about any possible attack / hacking of services, unauthorized access / attempt by Mental or external persons etc.			
119.	Resolution and restoration of services in case of any possible attack and necessary disaster management			
120.	Shutdown of critical services to prevent attack (internal or external)			
121.	Advise to improving network/Data Center security to protect NABARD's data / information from both internal and external persons/attack.			
122.	Resolution and restoration of services in case of any possible attack and necessary disaster management.			
123.	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as			
124.	And other related essential activities to ensure that the functionalities of IT Security.			
125.	Periodic reviews of domain level rights and privileges			
126.	Modifying access permissions and adding new access permissions of security policies on existing firewall.			
127.	Up-gradation of the firewall and IPS devices.			
128.	Signature update for IPS device.			
129.	Configuration backups for all security devices			
130.	Syslog server configuration & management including review of logs.			

131.	Managing / monitoring the IDS/IPS tool and policies as per guidelines of NABARD.			
132.	Modifying the policy for IDS/IPS/Firewall based on observed trends / security lapses.			
133.	Changing network address translation rules of existing security policies on the firewall.			
134.	Adding new network address translation rules on security policies on existing firewall.			
135.	Diagnosis and troubleshooting of the problem faced on firewall and faced by the IDS/IPS.			
136.	Managing / monitoring the IDS/IPS tool and policies			
137.	Periodic / Critical reporting to NABARD officials based on Firewall / IDS / IPS activities			
138.	Managing configuration and security of Demilitarized Zone (DMZ)			
139.	Alert / advise NABARD about any possible attack / hacking of services, unauthorized access / attempt by Mental or external persons etc.			
140.	Resolution and restoration of services in case of any possible attack and necessary disaster management			
141.	Shutdown of critical services to prevent attack (internal or external)			
142.	Advise to improving network/Data Center security to protect NABARD's data / information from both internal and external persons/attack.			
143.	Resolution and restoration of services in case of any possible attack and necessary disaster management.			
144.	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms			

	(single/multi factor), password policies such as			
Fortinet/Forcepoint/SDWAN Security Requirements				
145.	Install the security gateway in a distributed environment			
146.	Configure rules on Web and gateway servers			
147.	Create a basic rule base in Smart Dashboard and assign permissions			
148.	Schedule backups and seamless upgrades with minimal downtime			
149.	Monitor and troubleshoot IPS and common network traffic			

11. Data Base Administration

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
Database monitoring				
1.	Creating user-specific SQL or PL/SQL metrics with warning notification			
2.	Execution of user-specific scripts on Windows platform			
3.	Creating customized SQL reports with email notification			
4.	Dynamic visual indication of problems in the console			
Instance access to the following information				
5.	Size of databases			
6.	Free space in table spaces			
7.	User table spaces, spaces occupied by objects			
8.	Object/system privileges of users/roles, reasons of granting			
9.	List of roles/privileges granted according to a certain document			
10.	Description of users, their passwords, reasons for creation			
11.	List of scripts in a specific database and their purpose			
12.	Technical documentation of any database			

13.	Log of actions/crashes/incidents in any database			
Log of database changes				
14.	Date of creation/deletion of users/roles, log of privilege changes			
15.	Time of granting/revoking privileges, reasons for granting			
16.	Table space sizes			
17.	Time and date of database objects creation and deletion			
18.	History of database operations performed in the system (e.g., granting of privileges, creation of table spaces, etc.)			
19.	Connections to the database, with names of computers and solutions			
Automation of routine operations				
20.	Moving of tables. Automatic detection of available table spaces for moving			
21.	Automatic rebuilding of indexes invalidated during the moving of tables of their partitions			
22.	Quick creation of table spaces, automatic naming			
23.	Adding and resizing files, automatic naming			
24.	Splitting, exchange and removal of table partitions. Support of partitioning by various criteria (dates, interval)			
25.	Revocation of system or object privileges using lists User creation and editing			
Storage of documents and descriptions				
26.	Storage of database descriptions, their versions, paths, etc.			
27.	Descriptions of users and their passwords stored in an encrypted form			
28.	Comments to the privilege being granted (including the preferred revoking date to be monitored)			
29.	Comments to database files, table spaces, warnings			

30.	Action, crash or incident logs for each database			
31.	Descriptions of SQL and OS scripts, their relation to bases and hosts			
32.	Technical and work documentation on any database			
33.	Storage of database descriptions, their versions, paths, etc.			
34.	Descriptions of users and their passwords stored in an encrypted form			
35.	Technical and work documentation on any database			
Required Services				
36.	The DBA services shall cover existing production, testing & development DB environments that are in the organization at all locations.			
37.	New DB implementation , migration support and services& Services for Microsoft SQL 2012, 2016, 2019 , Oracle 11g , 12c, 19c, Mysql 7,8 , Postgres, PGsql & higher versions. Support and operation for any forthcoming application databases other than listed above.			
38.	–Specific activities only need to be handled by ITSM team. Enterprise application owners will be taking care of applications. Primary ownership will be with application owners and primary work to be done by enterprise application owners.			
39.	Change management of database schema, storage, disk space, table space, user roles, backup and purging etc.			
40.	As per IT security policy of the organization, ensure database patch management with minimum downtime and recommend appropriate patches of Operating System relevant to database.			

41.	Managing database upgrades operations. Including minor and major upgrades of all existing and newly introduced applications in future.			
42.	And other similar activities.			
43.	Advisory services to enhance application performance and user experience, user role management.			
44.	Proactive cleaning of extra tables.			
45.	Provide automation support.			
46.	Integration with different platform and systems.			
47.	Audit activity to be done frequently to review database schema, storage, disk space, table space, user roles, backup and purging etc.			
48.	The DBA services shall cover existing production, testing & development DB environments that are in the organization at all locations.			
49.	New DB implementation , migration support and services& Services for Microsoft SQL 2012, 2016, 2019 , Oracle 11g , 12c, 19c, Mysql 7,8 , Postgres, PGsql & higher versions. Support and operation for any forthcoming application databases other than listed above.			
50.	–Specific activities only need to be handled by ITSM team. Enterprise application owners will be taking care of applications. Primary ownership will be with application owners and primary work to be done by enterprise application owners.			
51.	Change management of database schema, storage, disk space, table space, user roles, backup and purging etc.			
52.	As per IT security policy of the organization, ensure database patch management with minimum downtime and recommend appropriate patches			

	of Operating System relevant to database.			
53.	Managing database upgrades operations. Including minor and major upgrades of all existing and newly introduced applications in future.			

12. Vendor Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Coordinate with vendors for support services.			
2.	Logging calls, tickets, coordination and follow-up with vendors			
3.	Escalation of calls to the higher levels at vendor side in case of requirement.			
4.	Vendor SLA tracking and monitoring with alerts and escalations (including WAN Vendor)			
5.	AMC/ Warranty/ Support Tracking			
6.	Providing necessary and advance information for entering into / renewal of AMC. (However, order and payment for AMC to the vendor will be made separately by NABARD)			
7.	Management of assets sent for repair.			
8.	Maintain database of the various vendors with details like contact person. Tel. Nos., escalation matrix,			

	and response time and resolution time commitments. Log calls with vendor Coordinate and			
9.	Analyze the performance of the vendor periodically (Quarterly basis or as specified).			
10	When a new solution (Hardware/software) is introduced, training to engineer/users to absorb and leverages the technology for business should be invariably arranged. And other related activities.			
11	End to end lifecycle management of new solution(Hardware/software)			

13. Help/Service Desk Services Management

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	Helpdesk resource should log all ticket received through various channels e.g. phone, email, IVR, sms, chatbot, MS-teams etc.			
2.	The Help desk team should be able to post the response back to the concerned people.			
3.	Helpdesk should classify and assign the ticket in appropriate section of ITSM services and other NABARD internal applications			
4.	Helpdesk tool should include tickets of all ITSM as well as NABARD internal applications and assign them to respective application teams.			
5.	If needed, the concerns/service requests can be escalated to concerned IT team who will be able to look into it.			
6.	Generate status report of pending/closed concerns on a daily/weekly/monthly basis.			

7.	Helpdesk should ensure that all calls to IT helpdesk are logged at a central helpdesk. All calls logged will have to be monitored and assigned to respective team /engineer / analysts and tracked for proper closure within the specified SLA limits. Helpdesk would ensure that the calls should be updated with			
8.	The service provider shall ensure that any change in resident engineers and/or helpdesk personnel is conveyed to the concerned NABARD officials one month in advance. The ITSM Service Provider would provide			
9.	The helpdesk shall provide support for distribution of computer peripherals on demand and			

14. Non-Delivery of Services / PENALTIES & SLAs

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	The tools provided for monitoring and managing these services should give a detailed report and Dashboard as per RFP			
2.	The total non-performance charges for a quarter will be calculated and deducted from the quarterly bill of the selected ITSM Service Provider. The report and Dashboard for all SLA breach should be available for NABARD			
3.	Penalty charges would be applied for those services, which have not achieved the stipulated service levels based on the table mentioned in Expected Service Delivery. There should be auto alert to NABARD in event of SLA breach.			
4.	Dashboard for Documentation and reporting as per SLA			

5.	Access to Dashboard/reports for the management users of the bank should be made available.			

15. Covering of absence of ITSM

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	The backup engineer in the centers should be trained in the presence of the main engineer and if need be, the backup engineer could be asked to manage the infrastructure in the supervision of the main engineer, for a couple of days. This will leads to a seamless backup of the main engineer when he avails of short spells of leave. Service provider should ensure that same engineer is available in absence of main engineer			

16. Staffing/Skill set/Qualification/Experience/Knowledge sharing:

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
Team Lead				
1.	MCA /B. Tech / BE			
2.	Mandatory certification: ITIL certified			
3.	Minimum 8 years of relevant experience as a IT Team Leader			
4.	Demonstrated service delivery experience & application support experience, preferably in a 24x7 environment			
5.	Experience in the use of an issue Logging, assigning and tracking system (Ticketing System)			
6.	Effective computer skills; Microsoft Office			
7.	Effective communication skills both verbally and in writing.			
8.	Experience of ITIL practices			

9.	Coordination with all technical teams for troubleshooting and RCA			
	IT Help Desk Executive			
1.	Minimum 3 years of relevant experience			
2.	Experience in IT helpdesk services			
3.	Basic understanding of computer technology in a business environment. Effective computer skills; Microsoft Office			
4.	MS outlook Email client, Helpdesk / Ticketing software applications.			
5.	Effective communication skills			
6.	Knowledge of ITIL processes			
7.				
8.	Relevant Experience - 5 years			
9.	Degree/Diploma in Computer Engineering, MCSE Certified, CCNA, RHCE, IBM AIX Administrator			
10	Experience in Windows Server 2008, 2012, 2016, 2019 and upcoming Versions Windows 10, 11 and upcoming Versions RHEL, CentOS, Ubuntu, Debian 7, 8, 9 and upcoming Versions. AIX v7 and above.			
11	Wide range trouble shooting skills involving, OS, Active Directory, LDAP, storage, security, DNS/ DHCP, DFS, printers, network, database, webserver management apache, tomcat, Jboss, IIS, Nginx, weblogic, websphere etc.			
12	Experience in Hyper-V, ESXi, Nutanix AHV, KVM hypervisors			
13	Experience with tower, Blade and Rack mounted workstations,			
14	Experience with thin clients (setup, configuration, and management)			
15	Experience managing, monitoring, scaling, and implementing large enterprise level virtual desktop and			

	application virtualization environments.			
16	Experience with disaster recovery of Microsoft Active Directory and Windows and Unix Servers			
17	Knowledge of storage technologies (NFS and iSCSI SAN, NAS)			
18	Linux (Suse, Red Hatt) Support			
19	Cisco/Virtualisation (Server & Desktop)			
20	Knowledge of storage technologies (NFS and iSCSI SAN, NAS), Linux (Suse, Red Hat, Ubuntu, AIX) support and Cisco/Brocade, Virtualisation (Server & Desktop)			
System Administrator Windows, Linux, AIX				
21	Degree/Diploma in Computer Engineering, MCSE Certified, CCNA, RHCE, IBM AIX Administrator			
22	Relevant Experience - 5 years			
23	Experience in Windows Server 2008, 2012, 2016, 2019 and upcoming Versions Windows 10, 11 and upcoming Versions RHEL, CentOS, Ubuntu, Debian 7, 8, 9 and upcoming Versions. AIX v7 and above.			
24	Wide range trouble shooting skills involving, OS, Active Directory, LDAP, storage, security, DNS/ DHCP, DFS, printers, network, database, webserver management apache, tomcat, Jboss, IIS, Nginx, weblogic, websphere etc.			
25	Experience in Hyper-V, ESXi, Nutanix AHV, KVM hypervisors			
26	Experience with tower, Blade and Rack mounted workstations,			
27	Experience with thin clients (setup, configuration, and management)			
28	Experience managing, monitoring, scaling, and implementing large enterprise level virtual desktop and			

	application virtualization environments.			
29	Experience with disaster recovery of Microsoft Active Directory and Windows and Unix Servers			
30	Knowledge of storage technologies (NFS and iSCSI SAN, NAS)			
31	Linux (Suse, Red Hatt) Support			
32	Cisco/Virtualisation (Server & Desktop)			
33	Knowledge of storage technologies (NFS and iSCSI SAN, NAS), Linux (Suse, Red Hat, Ubuntu, AIX) support and Cisco/Brocade, Virtualisation (Server & Desktop)			
	DBA Personnel - Oracle, MySQL			
34	BE/BTech/MCA			
35	Total experience: Minimum 5 years of post-qualification experience in Database management in Oracle DB 11g ,12c, 19c and higher. MySQL 7,8 and latest Relevant Database administration certified. Oracle certified DBA (OCP)			
36	Relevant Database administration certified			
	DBA Personnel - MS SQL, MySQL			
37	BE/BTech/MCA			
38	Total Experience: Minimum 5 years of post-qualification experience in Database management in MS SQL Server 2012,2014, 2016, 2019 and higher, relevant experience in MySQL, Postgres .			
39	Relevant Database administration certified. Microsoft Certified DBA (MCDBA)			
	Nutanix Administrator			
40	Nutanix certified professional (NCP MCI 5)			
41	Should have hands-on experience of 4 Years on Nutanix cluster installation, monitoring, maintenance and management			

42	VM Replication, Flow, LEAP, Xplay, disaster recovery.			
	Security Support			
43	BTech, B.E. / Graduate with relevant Experience - 2 years Fortinet Certified Network Security Administrator (FCNSA)			
44	Certified Forcepoint NGFW Administrator			
45	Check Point Certified Security Administrator (CCSA)			
46	Hands on experience in Maintaining a PSS environment.			
47	Hands-on experience on Firewall devices, VLAN, Proxy			
48	Reporting skills & good interpretation skills			
49	Excellent communication skills			
50	Knowledge on Network Security protocols			
	Network Engineer			
51	B Tech / Graduate in Computer Engg, E&C or Computer Application. , CCNA is compulsory. Juniper Networks Certification Program (JNCP), JNCIA-JunOS			
52	Total 2 years should be working as Network Engineer. Hands-On experience on big multisite LAN and WAN network.			
53	Should be able to solve all the monitoring part mentioned under Scope of work and should be able to act as first point of support for all DC/DR/HO/RO calls.			
	Backup Executive			
54	B Tech, B.E. / in Computer Engr E&C or equivalent			
55	Hands-on experience on high-end storage and tapes			
56	Hands-on experience on HPDP and Arcserve backup. Minimum of 3 years' experience is required in the relevant area			
	Regional / Corporate Office Service Support Engineer			
57	Graduation, Diploma in any discipline			

58	Certifications: CompTIA Network+, Network 5 Certification, Microsoft Certified Desktop Support Technician (MCDST) Microsoft Certified System Administrator windows 10 (MCSA)			
59	Two Years hands-on experience in installation and troubleshooting of windows operating system, application software's, peripheral devices and networking devices.			
60	Hands-on experience of basic networking.			
61	Working knowledge of ticketing system, ticket resolution and follow-up			
62	Working knowledge of online meeting setup and video conferencing, Teams and WebEx.			
63	Good verbal and written communication.			

17. General

1. SN	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
2.	Service period: NABARD intends to avail these services for a period of 5years and extendable by 1 year.			
3.	Knowledge Transfer and Handshake between existing and new ITSM Service Provider will be of 2 months from date of PO.			
4.	ITSM Service Provider will be responsible for all changes as per "Change Management Process" (Given in Annexure).			
5.	All resources will be appointed after screening / interview by NABARD.			
6.	All changes in ITSM resources should be informed to NABARD			

	one month in advance and NABARD will be part of all handover activities.			
7.	The ITSM Service Provider shall provide complete services as per the scope including mounting, unmounting, installation, implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.			
8.	The ITSM Service Provider shall ensure that during various phases of implementation, the performance, security, network availability, etc. of the existing network setup should not be compromised.			
9.	ITSM Service Provider shall provide a well-maintained Documents to NABARD			
10.	The ITSM Service Provider shall support for replacement and upgradation of out-of-support, out-of-service, end-of-life (EOL), end of support (EOS) undersized infrastructure elements as soon as the respective OEM announced the same at no additional cost to the bank throughout contract period. The ITSM Service Provider shall inform NABARD within 15 days of announcement.			
11.	The list mentioned above is the indicative list; however, the successful ITSM Service Provider should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the Bank.			
12.	The ITSM Service Provider shall adhere to the Service Level Agreements (SLA) and regular monitoring and reporting it to the bank.			

13.	The ITSM services should be compliant with Bank's IT, IS, e-mail and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.			
14.	The ITSM processes should comply with RBI cyber security circular no. RBI/2015-16/418 dated 2 June 2016 and its annexure 1- Baseline controls(including all relevant circular and update to same by RBI).			
15.	The ITSM process should be of ITIL 4.0 processes for Bank requirements related to change, incident, problem, configuration management, SLA and capacity management etc.			
16.	The ITSM Service Provider should follow a standard process to ensure that proposed solution meets functional, security performance and regulatory requirements of the bank. The selected ITSM Service Provider shall be responsible for proactive health monitoring of infrastructure on 24x7x365 basis.			
17.	The Bank has a complex infrastructure with multiple resources maintained and managed through multiple ITSM Service Providers. The ITSM Service Provider shall coordinate with all other ITSM Service Providers for seamless integration, implementation and operations			
18.	The ITSM Service Provider shall prepare the SOPs (Standard Operating Procedures) with periodical review as per industry practices and regulatory guidelines. The drafted SOPs shall be submitted to the Bank for its review and Approval.			

19.	The ITSM Service Provider shall configure the SLA Levels for all applications (including hardware & software) in IT Service Management tool with the functionality of auto-escalation of incident/ticket to appropriate bank authorities in case of breach of defined timelines for resolution of incident/ticket.			
20.	The ITSM Service Provider shall integrate all Bank assets (Servers, Storage, Network devices) in the monitoring tools and provide the unified Dashboard for monitoring & Management of devices.			
21.	The ITSM Service Provider shall be responsible for patching of Bank managed servers, all desktops connected in Bank network as per frequency of patches released by product OEM.			
22.	The ITSM Service Provider shall ensure patching & hardening for all Bank managed servers, and get the same cleared from the Information Security Cell /SOC of the Bank. The ITSM team has to prepare a patching calendar as per the frequency of the patch released by the OEM team and share the same with the bank team. The patches have to be applied in the same month in which OEM has released the patches as per prescribed as defined in SLA.			
23.	24 x 7 Support requirement with combination of onsite & offsite support. Onsite support is required for General shift(9AM to 6 PM) during normal working days. Support for remaining period is required on a call or remote basis. In case the issue cannot be resolved remotely, the SME (Subject matter expert) is			

	expected to travel to our site for support			
24.	VAPT support and compliance management (Review, General)			
25.	If required, for all scheduled and troubleshooting activities onsite engineers should be available on Saturdays/Sunday/Holidays			

18. Miscellaneous services

S N	Functional Compliance	Compliant as Out of Box functionality	Compliant with customization	Non compliance
1.	In the event of shifting of office premises / Data Centres / Disaster Recovery Centers / Near Disaster Recovery Centre by the Bank, ITSM Service Provider would depute Facility Managers / engineer(s) for de-installation of all the hardware, coordinate with 3rd party ITSM Service Providers, supervise packing/transportation and installation/ commission of equipment at new location. No extra cost will be borne by the Bank for the same. However, packing and transportation will be arranged by the Bank separately.			
2.	In the event of adding new office at new locations by the Bank, ITSM Service Provider has to assist the Bank in setting up of LAN (cabling, I/O fixing etc.) coordinate with network ITSM Service Provider for setting up of WAN connectivity etc. Cost towards raw material will be borne by the NABARD. As & when the Bank opens its new office it is the responsibility of the ITSM Service Provider to provide ITSM engineer on call basis as per the contracted rate.			

3.	Suggestions/ Recommendation to improve the current infrastructure architecture for better response & security.			
4.	ITSM Service Provider shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed in the Bank. The Bank will provide the list of all the authorized software and the number of licenses procured.			
5.	If Bank implements any project in future, then the ITSM Service Provider shall provide required support			

19. Own Geographical Spread

Sr No.	City	Functional Compliance		
		Physical office at NABARD office locations	Physical office at NABARD location is not present, however staff deputed for NABARD is on bidder payroll	Neither office at NABARD location is present, nor staff deputed for NABARD is on bidder payroll
1	Mumbai			
2	Port Blair			
3	Hyderabad			
4	Itanagar			
5	Guwahati			
6	Patna			
7	Raipur			
8	Goa			
9	Ahmedabad			
10	Chandigarh			
11	Shimla			
12	Jammu			

13	Ranchi			
14	Bangalore			
15	Thiruvananthapuram			
16	Bhopal			
17	Pune			
18	Imphal			
19	Shillong			
20	Aizawl			
21	Dimapur			
22	Delhi			
23	Bhubaneswar			
24	Jaipur			
25	Gangtok			
26	Chennai			
27	Agartala			
28	Lucknow			
29	Dehradun			
30	Kolkata			
31	Bolpur			
32	Mangalore			
33	Amravati			