REF NO. : PDCC/IT-Tender/2019-20/001 dated 19.06.2019 Date: 02.07.2019

Corrigendum - 1

For

REQUEST FOR PROPOSAL (RFP)

FOR

Selection of System Integrator for Core Banking Solution, Allied Applications and Related Underlying Hardware

THE PUNE DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

INFORMATION TECHNOLOGY DEPARTMENT

HEAD OFFICE: Pune District Central Co-op. Bank Ltd.,

B 4, B. J. Road, Pune.

Pin – 411001

Contents

Ref No. - PDCC/IT-Tender/2019-20/001 dated 19.06.2019

Corrigendum – 1 for Request for Proposal (RFP) for Selection of System Integrator for Core Banking Solution, Allied Applications and Related Underlying Hardware

In reference to the Request for Proposal (RFP) for System Integrator for Core Banking Solution, Allied Applications and Related Underlying Hardware, reference no. PDCC/IT-Tender/2019-20/001 dated 19.06.2019, all are advised to note following:

Section 1 Modifications in RFP Clauses

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
1	5.2.1	39	Multi Jurisdiction AML Compliance	RFP Clause stands deleted
2	5.2.1	39	Multi-Currency	RFP Clause stands deleted
3	5.2.4	40	Any other system as required by the Bank from time to time.	Any other system as required by the bank due to regulatory & statutory guidelines.
4	5.14 Disaster Recovery Centre (DR) on Hosting	75	Server Room Area g) The bidder shall provide adequate numbers of 32 amps industry standard sockets in single phase and adequate numbers of 64 amps industry standard sockets in three phase in Bank's rack space as per the layout.	Server Room Area g) The bidder shall provide adequate numbers of 32 amps industry standard sockets in single phase and adequate numbers of 64 amps industry standard sockets in Single/Three phase in Bank's rack space as per the layout & solution envisaged by the bidder.
5	8.14 Performance Bank Guarantee	114	1. As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable **Performance Bank Guarantee (PBG) for 5% of the total project cost** for 5 years 8 months(including 8 months transition phase) and valid for 69 months including claim period of 6 (six) months, validity starting from its date of issuance. The PBG may renewable year on year basis as per reducing balance of the total project cost. The PBG shall be submitted within 45 days of the Purchase Order from the Bank. 10. The Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee **(PBG) for 10% of the project cost** for YoY on reducing balance basis calculating actual payment received from the Bank and not on invoices produced (including 3 months transition phase) and valid for 69 months including claim period of 6 (six) months, validity starting from its date of issuance..	1. The Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) for 5% of the project cost for YoY on reducing balance basis calculating actual payment received from the Bank and not on invoices produced (including 3 months transition phase) and valid for 69 months including claim period of 6 (six) months, validity starting from its date of issuance..
6	Annexure 8.11 Section: HIPS		The application should support multiple approaches for vulnerability assessment, 1) Automated Vulnerability	RFP Clause stands deleted

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
			Assessment 2) Manual Vulnerability Assessment	
7	Annexure 8.11 Section: HIPS		Deep Packet Inspection (IDS/IPS) should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.	RFP Clause stands deleted
8	Annexure 8.11 Section: HIPS		Virtual Patching should be achieved by using a high-performance deep packet inspection engine to intelligently examine the content of network traffic entering and leaving hosts.	RFP Clause stands deleted
9	Annexure 8.11 Section: HIPS		Deep Packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.	RFP Clause stands deleted
10	Annexure 8.11 Section: HIPS		DPI should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities)	Solution should provide security monitoring across physical and virtual servers including real-time file integrity monitoring, anti-malware, configuration monitoring, and event logging and intrusion prevention.
11	Annexure 8.11 Section: HIPS		The solution OEM should deliver virtual patching updates after application vendor announcing a vulnerability in their system	RFP Clause stands deleted
12	Annexure 8.11 Section: HIPS		DPI should have Smart rules provide broad protection, and low-level insight, for servers and end-user systems. For operating systems and applications, the rules limit variations of elements of traffic, limiting the ability of attackers to investigate possible attack vectors since many attacks are based on exceeding expected characteristics. Smart rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.	RFP Clause stands deleted
13	Annexure 8.11 Section: HIPS		DPI should have Application Control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules will be used to identify malicious software accessing the network and provide insight into suspicious	RFP Clause stands deleted

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
			activities such as allowed protocols over unexpected ports (FTP traffic on a mail server, HTTP traffic on an unexpected server, or SSH traffic over SSL, etc.) which can be an indicator of malware or a compromise.	
14	Annexure 8.11 Section: HIPS		Solution should support creation of custom DPI rule.	Solution should support creation of custom rule.
15	Annexure 8.11 Section: WAF		The solution should be a Veracode VL4 certified to ensure that software is built using secure development practices	RFP Clause stands deleted
16	Annexure 8.11 Section: Anti DDoS		The proposed Equipment must make sure the DDOS mitigation devices can work independently when there is any problem happened in the DDOS detector.	RFP Clause stands deleted
17	Annexure 8.11 Section: Anti DDoS		The proposed system must be able to support netflow v5, netflow v9, sflow v4, sflow v5, netstream v5, ipfix for detection.	The proposed system must be able to support flow based detection or through device own detection engine.
18	Annexure 8.11 Section: Anti DDoS		Vendor should have received recommended ratings by NSS in latest NGFW report with a minimum exploit blocking rate of 99% & above.	Vendor should have received security recommended ratings by NSS in latest NGFW report with a minimum security block rate of 95% & above.
19	Annexure 8.11 Section: Firewall1		Solution should provide 6 Gbps of NG threat prevention throughput (includes Firewall, Application Visibility Web Filtering, IPS, AV, Anti-spyware, anti-APT etc. enabled)	Solution should provide minimum 6 Gbps of NG threat prevention throughput (includes Firewall, Application Visibility Web Filtering, IPS, AV, Anti-spyware, anti-APT etc. enabled)
20	Annexure 8.11 Section: Firewall1		The proposed solution of appliances should support the dynamic routing protocols OSPFv2 and v3, BGP, RIP, Multicasting PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3 etc.	The proposed solution of appliances should support the dynamic routing protocols OSPFv2 and v3, BGP, RIP, Multicasting PIM-SM, IGMP v1 and v2,etc.
21	Annexure 8.11 Section: Firewall1		The Firewall should support ISP link load balancing.	RFP Clause stands deleted
22	Annexure 8.11 Section: Firewall1		The Firewall should have integrated solution for SSL VPN.	RFP Clause stands deleted
23	Annexure 8.11 Section: Firewall1		It should support the authentication protocols RADIUS, LDAP, TACACS, and PKI-x.509 methods	It should support the authentication protocols LDAP, Radius/TACACS and PKI-x.509 methods
24	Annexure 8.11 Section: Firewall1		Should protect from DOS & DDOS attacks such as SYN Flood, UDP Flood, DNS Query flood and GET floods	RFP Clause stands deleted
25	Annexure 8.11 Section: Firewall1		IPS must have one-click single option to predefine action such as detect and prevent for newly signature downloaded in signature updates.	RFP Clause stands deleted

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
26	Annexure 8.11 Section: Firewall1		The AV engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware etc. using pattern based blocking at the gateways & should support both stream based & proxy based inspection capabilities to provide highest catch rate.	The AV engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware etc. using pattern based blocking at the gateways & should support stream based/proxy based inspection capabilities to provide highest catch rate.
27	Annexure 8.11 Section: Firewall1		The proposed solution should be able to detect & prevent the malware by scanning at least 20 different file types with configurable option to inspect, bypass or blocked various file-types as per organization need.	The proposed solution should be able to detect & prevent the malware by scanning different file types with configurable option to inspect, bypass or blocked various file-types as per organization need.
28	Annexure 8.11 Section: Firewall1		Users of LAN or WAN can go to internet through this firewall using web proxy as either transparent or non-transparent. Should provide a login facility to the users in accordance with scheduler wise web filtering control.	Users of LAN or WAN can go to internet through this firewall using web proxy /URL filtering. Should provide a login facility to the users in accordance with scheduler wise web filtering control.
29	Annexure 8.11 Section: Firewall1		Centralized Management should have centralized advance logging & reporting feature with at least 1 TB storage. In-case if inbuilt feature is not available. Vendor should provide additional external logging & reporting device.	Centralized Management should have centralized advance logging & reporting feature with at least 900 GB storage. In-case if inbuilt feature is not available. Vendor should provide additional external logging & reporting device.
30	Annexure 8.11 Section: Firewall1		Advance logging feature should have log indexing capability for faster log search & log optimization.	RFP Clause stands deleted
31	Annexure 8.11 Section: Firewall1		Should support for taking immediate action through logging pane in case of any critical DOS, Threat attempt.	RFP Clause stands deleted
32	Annexure 8.11 Section: Firewall1		It should provide a contained runtime Windows 32/64 bit virtualized environment such as WinXP, Win7, Win8.1, Win10 etc. to analyze threat & suspicious code and explore the full threat life cycle.	It should provide a contained runtime Windows 32/64 bit virtualized environment such as Win7, Win10 etc. to analyze threat & suspicious code and explore the full threat life cycle.
33	Annexure 8.11 Section: Firewall1		The solution should support at least but not limited to File types : - Archived: .tar, .gz, .tgz, .zip, .bz2, .cab, .rar,.7z,.tbz - Executable files (eg: .exe), PDF,.swf, Windows Office Document and Javascript	The solution should support all the commonly used File types
34	Annexure 8.11 Section: Firewall1		Should support emulation of at least 8000 files / per day.	Should support emulation of at least 1500 files / per day
35	Annexure 8 11 Section: EMS		It should have a secured single sign-on and unified console for all functions of components offered for seamless cross-functional navigation & launch	RFP Clause stands deleted

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
			for single pane of glass visibility across multiple areas of monitoring & management.	
36	Annexure 8 11 Section: EMS		The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems & Databases and Should be able to manage distributed, heterogeneous systems – Windows, UNIX & LINUX from a single management station.	The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems & Databases
37	Annexure 8 11 Section: EMS		The Tools must be able to measure systems availability and performance in near real time	The Tools must be able to measure systems availability and performance at least every 120 sec
38	Annexure 8 11 Section: EMS		The solution should have capability to monitor the systems by both agent-based and agentless mechanisms	The solution should have capability to monitor the systems by both agent-based /agentless mechanisms
39	Annexure 8 11 Section: EMS		The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes at least hourly basis; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
40	Annexure 8 11 Section: EMS		Proposed Service desk must be ITIL certified on at least 10+ processes.	Proposed Service desk must be ITIL certified on at least 4 processes.
41	Annexure 8 11 Section: EMS		Native integration of processes i.e. Incident Management with Change Management and vice-versa and also for Knowledge base i.e. automatically creation of knowledge base post closure of tickets	Native integration of processes i.e. Incident Management with Change Management and vice-versa
42	Annexure 8 11 Section: EMS		The tool should have well integrated listed modules - software asset management, contract management, finance management, procurement management	The tool should have well integrated listed modules - software asset management, contract management, procurement management
43	RFP Section 4: Eligibility Criteria	28		Additional Clause: The Prime Bidder can form a consortium maximum with two other partners for the overall scope of work defined in RFP.
44	RFP Section 5.3: Human Resource Management System	40		Human Resource Management System (HRMS) application has been dropped from Scope of work.
45	RFP : Scope of Work			The following applications are included as part of scope: i. PF TRUST

Ref No. - PDCC/IT-Tender/2019-20/001 dated 19.06.2019

Sl. No.	RFP Reference	Page No.	Original Version	Modified Version
				ii. Anti-virus for DC & DRC (Functional Specification mentioned in following section)
46	RFP : Scope of Work			The following interfaces are included as part of scope: i. BBPS ii. Unified Payment Interface(UPI)
47	RFP Section 3.2.1	12	NACH application- Application Provider: InfrasoftTech	NACH application- Application Provider: BSG
48	RFP	2	Last date of submission of the Technical and Commercial bid:: 12/07/2019 up to 15:00 hours	Last date of submission of the Technical and Commercial bid:: 24/07/2019 up to 15:00 hours
49	RFP	2	Date of opening of the Technical bid : 12/07/2019 15:30 hours	Date of opening of the Technical bid : 24/07/2019 15:30 hours

Section 2 Annexure 8.11 - Functional & Technical Infrastructure Specification

Minimum Technical Specifications for Anti-virus			
Sr. No.	**Particulars**	**Bidder's Compliance (F/N)**	**Bidder Remarks, if any**
1	The Solution should provide 5-layers of protection into a single agent -		
1.1	Network threat protection should analyze incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks.		
1.2	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits etc.		
1.3	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.		
1.4	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring more than 1000 file behaviors while they execute in real-time to determine file risk.		
1.5	Remediation and side effect repair engine should aggressively scans infected endpoints to locate Advanced Persistent Threats and remove tenacious malware. Administrator should remotely be able to trigger this and remedy the infection remotely from the management console.		
2	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.		
3	The solution should enhance protection for business critical systems by only allowing to run or by blocking blacklisted applications (known to be bad) from running. Finger printing of all applications should from centralized console.		
4	The solution should help prevent internal and external security breaches by monitoring application behavior and controlling file access, registry access, processes that are allowed to run, and devices information can be written to.		
5	The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system.		
6	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.		
7	The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources		
8	The solution should automatically engage in an aggressive scan mode if it detects large number of malware or high-risk threats on windows clients.		
9	The solution should auto-compile, auto-protect when the operating system kernel is not compatible with precompiled auto-protect kernel module especially for Linux variants.		
10	The solution should have incident investigation and response utilizing the integrated EDR capabilities in endpoint protection		
11	If any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediately install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etc.		

12	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.		
13	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.		
14	The solution must have reports that incorporate multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard.		
15	The solution must have group update provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.		
16	The solution should pre-emptively block exploits using heap spray techniques, abuse of java security manager etc. and must be signature-less and works regardless of flaw/bug/vulnerability		
17	Solution should collect and share the threat intelligence from / to external sources using industry formats such as STIX ,TAXII, etc.		
18	Solution should detect command and control traffic activity with IP level events, URL events, and DNS activity using detection mechanisms like static analysis, behavioral analysis, and reputation analysis from intelligence network.		
19	The solution should utilize multiple detection approach by combining virtualization and emulation to capture more malicious behavior across a wider range of custom environments.		
20	The solution should use a combination of static and dynamic analysis techniques to unmask cleverly disguised malware. It should detect packed malware and VM-aware ones that alter their behavior in an artificial environment.		
21	Solution should have dashboard to include the latest high risk tasks, search capabilities, recent samples, multiple processing stats, e.g. queue size, sandbox execution time, event count, tasks complete, and risk scores over say last 24 hours		
22	The solution must prevent clients from downloading full definition packages.		
23	The solution should manage single license for windows, linux and mac Operating Systems and management server should not be separate.		
24	The solution should detect malware that evades detection by using polymorphic custom packers by unpacking in a light weight virtual environment with no performance over-head.		
25	Solution should provide anomaly detection to detect and report on suspicious information found in a file. Preferable capabilities to include, TLS callback activity, CVE and exploit detection, shell-code detection, debugger detection, watermark tampering, and non-standard file alignment, RFC compliant etc.		
26	The solution should set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed.		
27	The Solution should provide manage windows, Linux and mac agents from same centralized console.		
28	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth		
29	If the endpoint client detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer		

30	The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources		
31	The Solution must have a layer of protection that enables organization to go on the offensive and lure attackers out of hiding and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.		
32	The solution should provide incident investigation and response utilizing the EDR capabilities in endpoint.		
33	The solution's EDR should be able expose advanced attacks with precision machine learning, behavioral analytics and threat intelligence minimizing false positives.		
34	The Solution should provide report over email, CSV, html or pdf.		
35	The solution should be in the leaders quadrant of latest Gartner Report for endpoint security.		
36	Solution should be able to do Real time virus detection, cleaning/quarantine.		
37	Solution should be able to do Heuristic scanning to allow rule-based detection of unknown viruses.		
38	Solution should be able to quarantine files and files should be available in Quarantine Manager.		
39	Scanning of compressed file archives in ZIP, JAR etc. formats. Protection from viruses hiding in compressed files, such as Internet downloads and e-mail attachments.		
40	Solution should be able to do Proactive protection against zero-day threats.		
41	Solution should have the Facility of Vulnerability analysis tool.		
42	Solution should have the ability to Scan CD ROM and other external Drives automatically in real-time when accessed.		
43	Solution should have functionality of Central management console to centrally control desktop configurations, including scanning and cleaning options.		
44	Solution should have Centralized Audit trail logging and reporting capability with ability to communicate the reports using email.		
45	Solution should have Role based administration of the solution.		
46	Solution should have the ability to Real-time lock down of client configuration - allow or prevent users from changing setting or unloading/uninstalling the software.		
47	Solution should Automatic downloads of latest virus signature updates from the Internet to desktops and servers, across different platform running Windows. The distribution should happen seamlessly from a single management console.		
48	Solution should Remote deployment of Client software using Web- based installation/remote installation/ Log-in script/Client Packager.		
49	Solution should have ability to force an update (PUSH) to client.		
50	Solution should have an in built feature for Device control.		
51	Solution should Support for additional features like Desktop Firewall, Intrusion Prevention System etc.		
52	Solution should support Parental Control application.		
53	Solution should have 24x7 Technical Customer Care Support.		
54	The Antivirus must be compatible/support to run on Operating systems like Windows server 2012/2016.		
55	Antivirus should protect their own program files.		
56	Reporting of total system information to troubleshoot the problems and Web based Secured Management Console.		

57	Solution should Block auto play of USB device.		
58	The Antivirus solution must be able to auto quarantine or auto delete spyware without end user intervention.		
59	Prevent malicious website and prevent dangerous downloads from spreading malware & SPAM.		
60	Endpoint should Detect attackers by luring them into a decoy minefield		
61	Endpoint should Coax them into revealing their intent, tactics, and targets–so you can adapt your security posture.		
62	Endpoint should Bait the trap by simply flipping a switch.		
63	Endpoint solution should Lock down endpoints by specifying which applications can/cannot run with smart Application Control.		
64	Enable safe download and use of any app with Application Isolation		
65	Beat crippling ransomware and unknown attacks with a combination of signature less and critical endpoint technologies.		
66	Maximize protection and minimize false positives with machine learning technologies		
67	Block zero-day attacks that prey on memory-based vulnerabilities in popular applications.		
68	Solution should have a single agent for Anti-Virus and EDR capability		

Minimum Specifications for PF Trust			
Sr. No.	**Particulars**	**Bidder's Compliance (F/C/N)**	**Bidder Remarks, if any**
1	**General UI Requirements**		
1.01	The system should have a browser based interface for entire functionality provided to PF Office of PDCC		
1.02	The system should have dropdown list selection for select fields/ lookup values; entry list must be able to limit entry to only valid values.		
1.03	The system should have help text, by screen and by field.		
1.04	The system should have availability of online help, including illustrations, tutorials and reference materials.		
1.05	The system should have intuitive query / filter facility that is easy to learn and easy to use by nontechnical personnel.		
1.06	The system should have Scroll (with a single keystroke) forward, backward, up and down for multiple screen displays.		
1.07	The system should have Hot key for common screen transitions		
1.08	The system must provide a facility for generating and viewing reports for transactions handled during a specified period (daily, weekly, monthly, yearly and any user defined period).		
1.09	The system should support both graphical and textual output		
1.10	The system should provide MIS reporting with multiple "Slice & Dice" options to generate reports in flexible formats based on user specific needs.		
1.11	The system should be able to model a reporting format.		
1.12	The system should provide a facility to create custom queries and reports that can be stored, reused, printed and emailed.		
1.13	The system should have provision for immediate and scheduled batch reporting.		

1.14	The system should provide flexible (custom) report creation capabilities such as user definable data selection criteria, user definable columns and headings		
1.15	The system should support graphical reports.		
2	**CIF & PF Savings Account Opening**		
2.01	System to capture Customer Information Form (CIF) details as followed in PF Fund Office at PDCC Bank		
2.02	System should have the ability to do a de-duplication check for KYC purposes like PAN, Passport No., Aadhar, Voter ID, Other ID / Address Proof.		
2.03	System to apply necessary validation in Customer Creation Forms to avoid incorrect recording of data in the customer id opening		
2.04	System to Capture Customer ID and get details from CIF. Allow entry for new PF Fund Savings accounts.		
2.05	System to apply necessary validation in Account Opening Forms to avoid incorrect recording of data in the account opening		
2.06	Provide for existing account check for all accounts related to the customer in the PF Fund Office (e.g. first name + last name, passport number, PAN card number, telephone number, voters ID, combination of any etc.)		
2.07	System to enter special instructions (if any)		
2.08	Allow for the flexibility to have both a passbook and a printed statement		
2.09	Capture the frequency for account statement printing / mailing / faxing including email		
‘2.10	System to define MIS Reports/statements which will be generated on defined events (on opening of an account, at the day end) or at any given time for accounts opened.		
2.11	Allow bank-defined number of nominees to be nominated by the account holder. Capture the following minimum details for each Nominee VIZ. Name, Address, Telephone number, Relationship with account holder, Date of Birth, Proportion of available balance that each nominee is eligible for etc.		
2.12	Deceased Account		
2.13	System to restrict a user from adding any nominee after an account has been marked as "Deceased" Account Holder.		
2.14	Signature scanning/capturing facility. There should be no limit on the number of signatures that can be scanned and stored for a particular type of account. System should have provision for capturing full signature at the customer level and specimen signatures at the account level of the customers.		
2.15	System to maintain a history all signatures for a particular customer ID / account. Viewing shall be restricted to signatures marked current.		
2.16	Photo scanning/capturing facility and it should be kept in secured environment not accessible for ordinary user from inside outside the system. Should also be able to replace		
2.17	System to allow PF Fund Savings account for the staff as per product features, rules to operative this account AS followed in PF Office at PDCC Bank.		
2.18	System to define interest application, calculation frequency and for example weekly, monthly, quarterly etc. as defined in the interest calculation module		
2.19	System to define the method of interest calculation for example simple, compounded etc.		
2.2	System to define business rules for interest calculation if partial withdrawals of the PF is done by the member from its PF Account. This configuration shall be as per the product rules followed at PDCC Bank PF Office		

2.21	System to generate demand for deduction of monthly PF amount to be sent to PDCC Bank Payroll Section		
3	**PF Loans Account**		
3.01	System to allow defining various Loan Products by PF office for it members. The various loan products includes 'Home Loan', 'Personal Loan', 'Education Loan', 'Vehicle Loan' etc.		
3.02	System to capture various Input Fields for creation of Loan Accounts viz. Customer Id, Acct Opening Date, Interest Rate, Loan Amount, Loan Period, Loan Product / scheme, Amortization Chart etc.		
3.03	System should facilitate various loans related transactions viz Disbursements, Charges Posting, Recovery, Interest Calculation, Interest Posting, Demand Generation etc.		
3.04	System should generate all Loan related reports viz.: Loan Summary Report, Individual Loan Report with Loan History, Interest Calculation Report, Received Interest Report,		
4	**Investments**		
4.01	System to allow recording various investments made by PF Fund. The various investment types (but not limited) includes Government Securities, Shares Investment, Mutual Funds, Call Money Deposits, Term Deposits		
4.02	System to allow recording of applicable field information for various investment types viz.: Transaction Date, Investment Period, Interest calculation date, Investment Name, Investment Amount, Interest Rate and calculation		
4.03	System to generate Investment Reports such as investment summary report, invest type wise report, investment scheme wise report		
4.04	System to perform periodic interest calculation, interest posting on investment accounts		
4.05	System to generate various investment interest reports viz. 'interest calculation report', 'received interest report', 'accrued / suspense interest report', 'interest receivable report' etc.		
4.06	System should have necessary validations in place to avoid incorrect data recording into the system.		
5	**General Accounting/Financial Management**		
5.01	System should allow to record input transactions viz. Receipt Vouchers, Payment Vouchers, Journal Vouchers etc.		
5.02	System should generate various reports related to receipt, payment and journal entries		
5.03	System should generate various ledger reports i.e. individual account ledger and summary reports.		
5.04	System should generate various financial statements viz. Trial Balance/Profit & loss/Balance Sheet		
5.05	System should have inbuilt functionality of bank reconciliation for the bank current accounts of PF Office in other banks.		
5.06	System should generate necessary Accounting and Financial Management Reporting		
5.07	System should generate various ratios and ratio analysis, on the basis of financing management data.		
5.08	System should provide interface for graphical analysis, on the basis of financing management data.		
5.09	System should have facility to calculate and deduct TDS as per rules.		
′5.10	The system shall have separate menu to enter the opening balance or it shall carry forward the closing balance of previous years automatically.		

5.11	The system should have facility to open the multiple financial year and login into older financial years to only view reports in that financial year. The transactions posting should not be allowed in previous financial years.		
5.12	The system should have maker-check facility for all financial transactions.		
5.13	The system should have facility to maintain the advances / imprest taken by staff. The system should have facility to record expense voucher against the advance taken.		
5.14	The system should have facility to record daily office related expenditure viz.: Travelling daily allowances, Postage and Telephone, Fuel, Stationery and Printing, Repair and Maintenance, Utility (electricity/water) charges, Insurance (Property) premium, Bank Charges etc.		
5.15	The system should have facility to enter transaction in one-to-one batch or one-to-many batch;		
5.16	The system should have facility to create template for repetitive batches.		
5.17	The system should have inbuilt fixed assets management system to record Fixed Asset Details, Capital Expenditure transactions, depreciation calculation, etc.		
5.18	The system should have facility to generate necessary reports in Fixed Assets related masters and transactions.		
6	**User Management:**		
6.01	The system should facilitate a) Creation and management of unique keys for identities b) Configurable generation of unique logins		
6.02	The system should provide password management through both administrator and end-user (Self Reset)		
6.03	The system should facilitate creation of user roles and assigning menu level rights to user role.		
6.04	The system should facilitate creation of user logins.		
6.05	The system should facilitate assigning menu access rights to users by assigning the User role to User; Adding, removing specific menu rights to users after assignment of user role to the user.		
6.06	The system should maintain log of all entry, update, deletion activities made by the logged in user.		

On-premises Email Solution			
Sr. No.	**Particulars**	**Bidder's Compliance (F/C/N)**	**Bidder Remarks, if any**
1	The Bidder/ OEM must have successfully Supplied & Installed the proposed IDN Complied solution for atleast 2 government or PSU accounts for min. Ten thousand mailboxes out of which atleast one must be have email address created on English along with any local language domain i.e. Marathi , Hindi etc.		
2	The proposed solution should have production instance in DC only but the production data should be backed up at DR. The solution should have 2000 users and 95% mail box should have allocated space of 100MB/mailbox and rest 5% should have allocated space of 1 GB/mailbox		
	IDN Complied Email Solution		

3	The solution should support industry standard protocols: IPv4, IPv6, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, HTTP, HTTPS, SSL v3.0, TLS 1.0, 1.1, 1.2, UNICODE and SNMP (log management).		
4	The solution should support IDN (at least Marathi (मराठी) Hindi (हिंदी) and EAI (email address internationalization). The Solution should support creation of email addresses on IDN domain name and Marathi/Hindi mail boxes from day one. Both email address should be usable in one single login email interface.		
5	The solution should support the deployment of messaging sub-systems/ components on multiple physical/virtual servers (Intel architecture) each performing a specific role.		
6	The solution should support integration with leading third-party storage Sub systems (both SAN and NAS).		
7	The solution should be scalable i.e. both Horizontally and Vertically and should also support HA architecture.		
8	The solution should also provide its own backup/ restore mechanism OR alternatively should support leading third-party Backup solutions from VERITAS/ IBM/ EMC/ HP etc.		
9	The solution should support integration with own/ third-part AV, Anti-Spam, Anti-Phishing solution.		
10	The solution should support multi-tenant architecture i.e. hosting multiple domains as per requirement.		
11	The solution should support native as well as LDAP v3 authentication (MS-Active Directory)		
12	The solution should support programmatic mailbox creation & contacts management (both from .Net and JAVA applications).		
13	The solution should include a user-friendly HTTP and HTTPS based Web Email client capable of performing all standard Email functions including Address book Import & Export, Signatures, Automatic replies, Read-receipts etc. The web mail client should be supported on leading desktop/ laptop browsers (IE, Chrome, Firefox, Safari on MAC) including smartphone and tablet (Android, IOS, Windows). SSL certificate shall be provided by bank.		
14	The Web Email Client login interface should be customizable (for branding).		
15	The solution should support third-party mail client software (both IMAP/ IMAPS and POP3/ POP3S based) like MS-Windows Mail, MS-Outlook, iOS Mail, Thunderbird etc.		
16	The solution should include a user-friendly HTTPS based web interface for Mail Admin & Support team for performing centralized admin and support functions based on the assigned role. The web interface should be supported on leading desktop/ laptop browsers (IE, Chrome, Firefox, Safari on MAC) including smartphone and tablet (Android, IOS, Windows). SSL certificate shall be provided by Bank		
17	The solution should allow admin to define the mailbox quota on per-user basis and should also allow to set the expiry date of a user mailbox.		
18	The solution should not have any limitation on no. of mailbox/ user creation i.e. no user/ mailbox based licensing.		
19	The solution should provide standard reports (CSV/ XLS/ XLSX, PDF and HTML formats) on mail usage including server health, top mail users, mailbox statistics etc.		
20	The Solution in its web based login should have inbuilt capability of PGP Encryption (Pretty Good Privacy) to send and receive Encrypted emails.		

21	The Solution in its web based login should have capability to give access of your account, authorize your subordinates or your agents to receive your emails. they can reply on those mails on your behalf without sharing login credentials of your account.		
22	The Solution in its web based login should have Snooze capability to allows an user to temporarily disappear email for a user defined time from inbox and make it appear as a fresh email in the inbox on defined date & time.		
23	The Solution should have Homograph attack prevention and Downgrading - Backward capability: Help to deliver all your emails to non EAI ready email		
24	The solution should offer Devise Specific Access Control feature so that users who are not allowed to access their accounts on different devises due to security reasons and be controlled.		
25	The solution should offer Dual Step Authentication SMS Based or XCODE: By enabling Dual Authentication we can keep unauthorized users away from our account & hackers cannot login in to our account. Xcode allows us to login without SMS/ mobile		
26	The solution should offer Country Specific Access Control so that admin can implement policy that users of organization, can access their account in different geographic locations or not.		
27	The solution must provide SOAP API – which will be required in case of any integrate with ERP or Website / Transactional Emails and store them into		
	IDN Complied Mail Security & MX Gateway Solution.		
28	The Solution should be EAI (email address internationalization) ready and must support IDN .bharat (.भारत) domains for sending and receiving emails from email address using IDN domains.		
29	The solution should block SPAM (both inbound and outbound) emails.		
30	The solution should be configurable on any TCP port defined by the		
31	The solution should have antivirus engine which detects viruses, worms and trojans, including Microsoft Office macro viruses, mobile malware, and other threats. Built-in support for various archive formats, including Zip,RAR, Tar, Gzip, Bzip2, ELF executables, Portable Executable, popular document formats including MS Office, HTML, RTF and PDF files. It should also allow additional file extension blocking facility as per requirements.		
32	Safe hold place for spam mails, manageable by users and administrator. It should provide Quarantine and Blocking facility.		
33	The solution should have a secure Web based login for remote administration.		
34	The solution must have powerful logging to enable administrators and support persons to track each and every email.		
35	The solution should be able to perform loop detection and drop the connection if loop is detected.		
36	Scalable Solution: The solution should be scalable to lakhs of users just by adding new nodes.		
37	Transport Layer Security is a security measure to safeguard emails while flowing between servers. TLS encrypts emails while in transit. This way it is impossible for a sniffer to see contents of email. If an external email server supports TLS, solution must always send the email using TLS. Only if that fails, the email should be sent as unencrypted.		
38	The solution should offer routing/ firewalling capabilities and should be able to redirect the deliveries of the email on the basis of From ID or To ID, Sender Domain, Recipient Domain etc.		

39	The solution should be capable of validating the Reverse DNS, MX, SPF, A record of the inbound mail domain.		
40	The solution should also have some Challenge-Response mechanism for False positive handling		
41	The solution should check senders IP address against blacklisted IPs in real-time		
42	The solution should allow the administrator to Whitelist/ Blacklist any IP, domain or Email Address.		
43	The solution should allow to create exceptions for specific users/ groups.		
44	The solution should support message size restrictions for each configured domain.		
45	The proposed solution must support verification of user i.e. user existence on the email server before accepting any mail.		
46	The solution should support SSL (SSL certificate shall be provided by RISL).		
47	The solution should support SMTP-AUTH as defined in RFC 2554.		
48	The solution should support authenticated SMTP service and does not allow emails to be sent as 'From internal domain' without the successful authentication.		
49	The solution should validate the From/To addresses of outgoing emails to make sure that they are valid email addresses.		
50	If any internal user sends a new SPAM and significant number of complaints is received against the Email, the user email address should be blocked from sending out emails. Incoming emails for the user is still functional and accessible. The solution should support this capability.		
51	If a user's password is hacked/ compromised and SPAM is sent through the account, Outgoing Email privilege of the user should be automatically blocked and alert should be sent to Administrator.		
52	The solution should have Email Digest capability i.e. a web based interface should be provided for searching the blocked Emails (both Inbound and Outbound).		

Section 3 Annexure 8.12 – Commercial Bill of Material

Please refer attached revised **Annexure 8.12 – Commercial Bill of Material.**