पेंशन निधि विनियामक और
विकास प्राधिकरण
बी-14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली-110016.
दूरभाष : 011-26517501, 26517503, 26133730
फैक्स : 011-26517507
वेबसाइट : www.pfrda.org.in

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY
B-14/A, Chhatrapati Shivaji Bhawan,
Qutab Institutional Area,
Katwaria Sarai, New Delhi-110016.
Ph : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

Circular

No: PFRDA/2020/21/REG-CRA/2

Date:15.06.2020

Guidelines related to Functional, Technical & General Specifications /Criteria to be considered while processing applications for Central Recordkeeping Agency (See reg. 4(d)

In reference to terms of proviso (d) of regulation 4 of Pension Fund Regulatory and Development Authority (Central Recordkeeping Agency) (First Amendment) Regulations, 2018, notified w.e.f 25.06.2018. Authority hereby prescribes the outline of functional, technical and general specification under below points –

1. Building of Infrastructure
2. Setting up of Infrastructure
3. Scope of work of CRA services
4. Service Level Requirement
5. Deliverables and Project Schedule
6. Technical Proposal Format

Establishment and Operationalization of CRA

Objective: CRA System designing, development, implementation and maintenance

Summary of Technical requirements:

Modern Application: New generation software solution.

Open Architecture: Platform architecture should be open, flexible and dynamic in nature.

Ease of Maintenance: The solution should be modular and configurable for ease of change management and maintenance while providing the flexibility of accommodating

new generation application.

High Availability: The application should have 99.5% availability. It should allow online addition, deletion and modification of the software modules without any impact on aforesaid availability.

BCP: The system should support a Recovery Point Objective (RPO) of zero and Recovery Time Objective (RTO) of near zero.

Scalability: The system should provide horizontal, vertical and linear scalability without inherent bottle necks and design changes. The solution scalability should be proven by carrying out the benchmark exercise by applicant.

Configurability: The system should be highly configurable and parameterized.

High Capacity and Throughput: The solution should have high throughput and capacity; a solution capable of achieving a sustained throughput of 1000 Transactions Per Second (TPS) to be provided to start with. Application should be scalable to handle a throughput of 5,000 TPS and above to meet future requirements.

Platform Independence: The solution should be Platform independent and should not be constrained to a single Hardware Platform or Operating System or database.

Monitoring Capability: The solution must have adequate real-time monitoring of the transactions and application modules with automated alert mechanism through multiple channels.

Secured: The CRA System has to be developed from approach of "secure from start" and should have all controls well defined as per regulator, industry standards (Data Security Standards, ISO) requirements and PFRDA Policies.

Natively IPv6 Ready and Backward Compatible.

Overview of Requirements: The applicant is expected to build necessary infrastructure for providing CRA services to various stakeholders. The services, applications and infrastructure required for this purpose are depicted in the diagram given below.

It is proposed that the establishments and operationalization would be undertaken viz. building of infrastructure, operations and maintenance, and termination phase. The broad scope of the activities is described below.

1 Building of Infrastructure

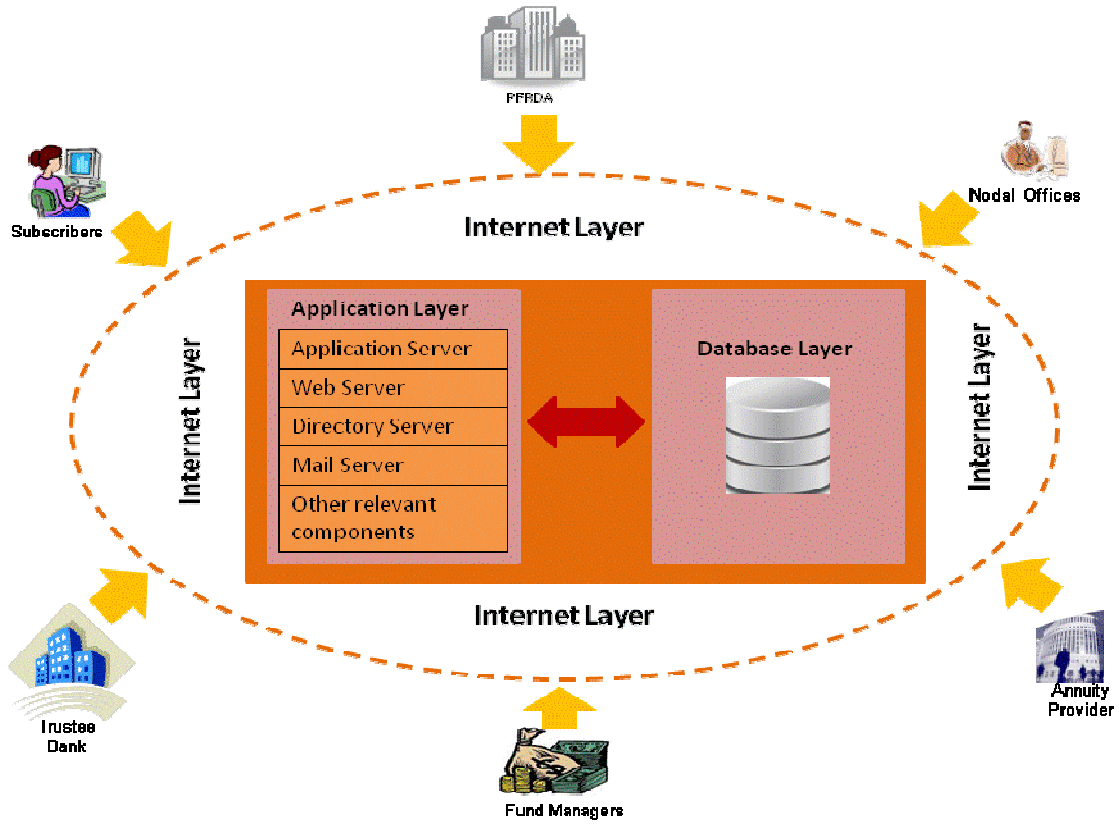
This involves building necessary IT infrastructure considering the requirements and Service level (SL) parameters specified. This broadly involves

i. Application development

- SRS preparation
- Application development and implementation
- User Acceptance Test

ii. Application Architecture

The application architecture of the solution should be one which not only fulfills the role of providing services to stake holders but also takes into account scalability in terms of growth of users, increase of stakeholders and increase in services offered by National Pension System (NPS). Pension data being financial data of the public and their life's savings, security and confidentiality forms a crucial consideration. Also, the system is critical and needs accessibility and flexibility in terms of inter-operations with other systems. Hence, it is emphasized that the applicant should develop a technical solution considering these requirements and challenges. The broad architecture in terms of technology is illustrated in the diagram below. In nutshell the architecture should conform to open standards.



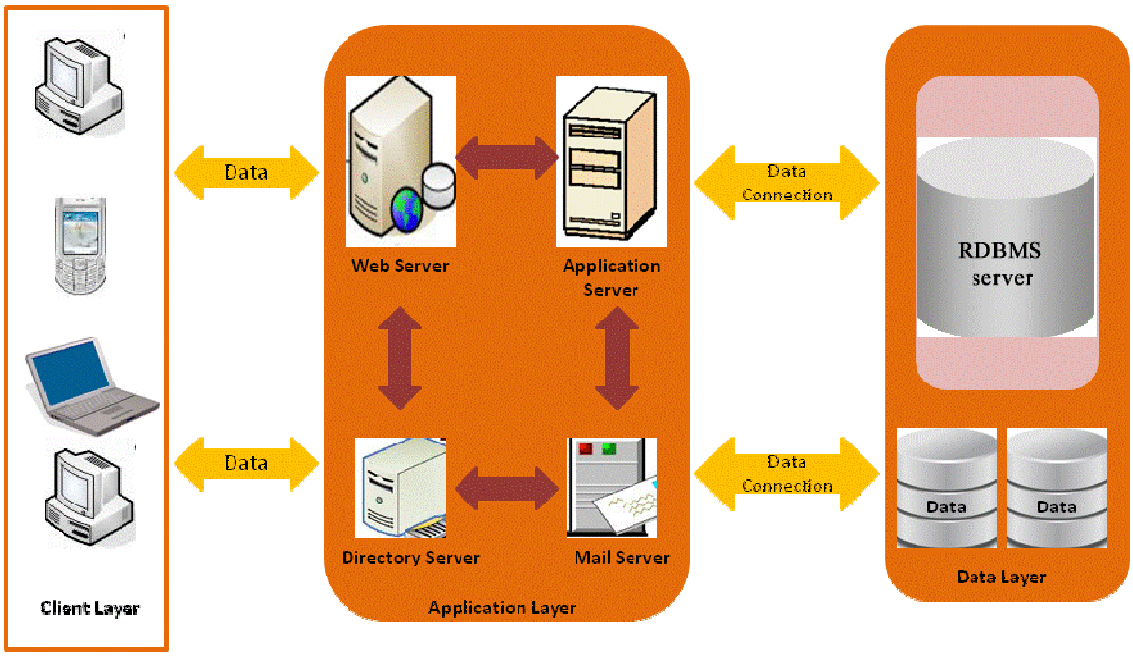
Considering the diverse functional requirements, the sub architectures can be categorized as under

- The application sub architecture
- The data management sub architecture

(a) Application sub Architecture

Application sub architecture describes the technology and standards that facilitate communication and functional interface between systems, both at module-to-module level or intra-application level, and at the application-to-application or inter-application level. The application sub architecture domain therefore encompasses the aspects of communication (inter and intra-application) and integration. The scope is to provide a framework under which the CRA application system can be integrated to improve service delivery and business value. These are indicative guidelines, however, the applicant is expected to arrive at an appropriate solution.

The diagram below shows the application sub architecture. The suggested components would be as follows:



Application Server: This is the main application engine where the core application will be hosted.This will provide the core functionalities and will be connected to the database layer.

Web Server: The solution is a web based application, therefore, a web server component is necessary for hosting.

Directory Server: The system is expected to have a single sign on The directory server is to facilitate this function and allow for Single sign on services.
Mail/Messaging Server: This component will take care of the mail and messaging needs of the application. The major chunk of communications will be through e-mails and messages.

(b) Data Management sub Architecture

This architecture covers the business and technical aspects of managing data and the database environment. The structure of the data management system should reflect a lifecycle approach to data management such as collection from the end users, analysis and planning, acquisition, use, operation and maintenance, archiving and disposal. The data management framework encompasses business rules to ensure the security and consistency of data. The system should:

- Provide the NPS with a framework for best practices in data management
- Facilitate effective management of NPS data within legislative and regulatory guidelines.
- Provide highly secure environment for storing the data

iii. Data Management Framework Requirements (Data transfer pertaining to the PRANs opting for CRA)

- Preparation of Data Migration (Transfer) strategy
- Data Migration (Transfer) for interoperability
- System driven co-ordination of data.

As data is the most critical component of the entire solution, it is emphasized that a data management framework should be in place for the proper use of data. This should not only consist of the technical infrastructure, but also the proper manpower and security infrastructure**.**

- Data management activities should be planned and governed, based upon business needs with relevance to the highly critical and sensitive nature of the NPS data
- Data should be acquired, updated and catalogued in a coordinated manner and in accordance with agreed standards regarding acquisition, access, storage and dissemination.
- There should be a policy framework, mechanisms, audit procedures and training in

the CRA for proper use of the data. At every step, representatives of the PFRDA have the right to check these mechanisms and have their comments incorporated

- The database should be established for ensuring data integrity, risk management and availability.
- The data should be archived and disposed of in accordance with best practices and security guidelines.
- The applicant should have an established data management framework that ensures effective storage, retrieval, access, sharing, privacy and security are maintained for operational processing and analysis.
- There should be accountability for data management.
- In this context, it should maintain regimes for data integrity, data identification and maintain an inventory of all data holdings.
- It should account for the value and expected lifespan of the data assets.
- It should have metadata repositories, which provide details of location, content and business purpose.
- The CRA should have a coordinated and published plan and means for data capture.
- It should be able to implement an integrated data coordination framework to leverage existing systems in data acquisition and holding.
- It should provide clear communication and education regarding proper and improper use of data.

The applicant should have clear formulated policies regarding the items mentioned below which will form the basis of their data management solution:

- Use of data in transactional and analytical processing
- Brokerage, duplication and partitioning
- Use of data in management support systems and data warehouses
- Authoritative source and instances of data records
- Database management systems and open standards
- Backup and recovery
- Access management
- Data integration
    - ❖ Replication and warehousing
    - ❖ Data archival and disposal in accordance with relevant legislation, standards and guidelines
- It should ensure that business data access and usage is audited.

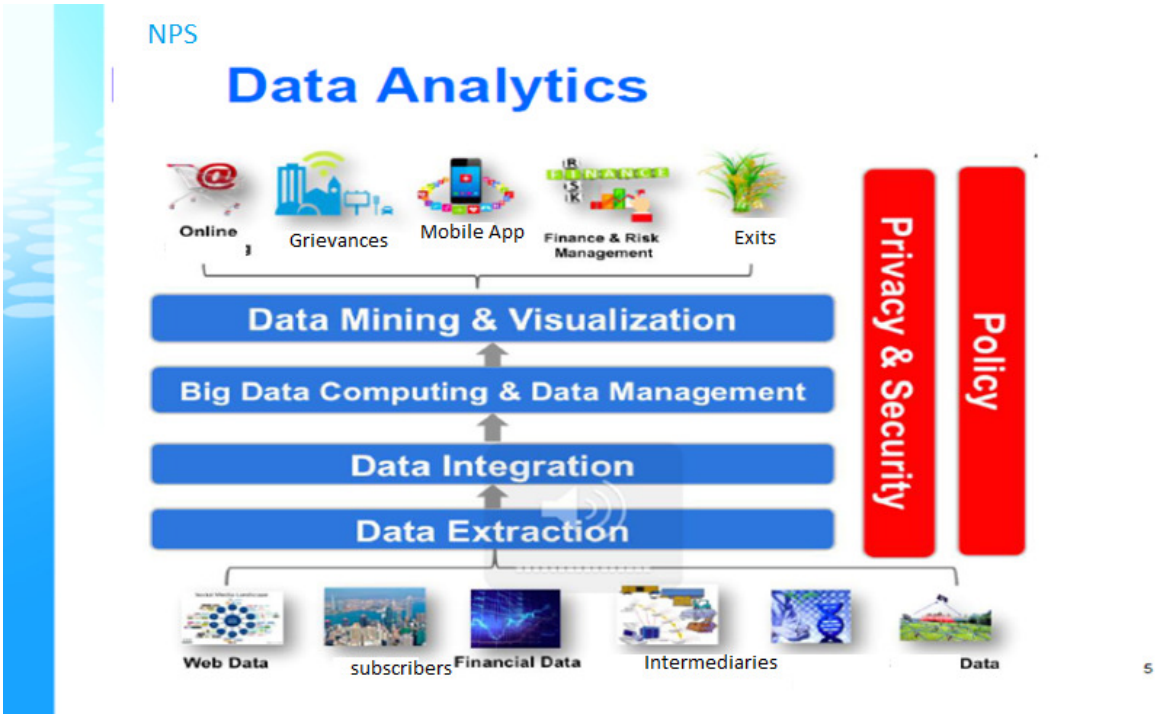
- It should document and implement current architectures and procedures for data operations and maintenance.

The database server proposed should be among the best of the breed and comparable to all the other major database servers. The proposed product should at least meet the below mentioned criteria:

- RDBMS product
- Provide extensive support for transaction processing (ACID properties)
- Direct Unicode support
- Conform to open standards
- In-built support for storage of binary objects and XML
- ODBC and JDBC Support
- Easy to use tools for designing and export / import

The system shall have facility/capability of transmitting and receiving data to and from the existing CRA/CRA's including interconnectivity for migration of data and or information. The interoperability function as provided above shall be built in co-ordination with the existing CRA and in case of any dispute on any related matter between the CRA's, the decision of PFRDA shall be final and binding on all parties concerned.

Pension Data Analytics



(iv) Expected Minimum Performance Requirements from Application and Platform

Availability	Scalability	Security	Interoperability	Maintenance	Performance	Extendibility	Reliability
The application should be available 99.5% of the time during 8 am to 8 pm and 97.5 % during the remaining time of the day.		The system should have strong role based access control logic built in it. Access control mechanism should be at multi levels	The application should be interoperable between platforms.	Follow standard IT management Framework such as ITSM.	Response time should be no more than 7 seconds for any query/posting.	Application should take not more than 90 man days for extension /upgrade/ interfacing for interoperability	The Mean Time Between Failure should be more than 24*30*3 hrs
All routine maintenance downtime should be announced and intimated to the PFRDA at least 120 hours in advance and		The solution should provide Single-Sign-On features with password encryption protocol and capability to enforce	The system should use open standards for inter operations and for data interchange	The provider should update patches and upgrades to the operating system within a month of release	There should be performance tuning every 6 months	The system should allow for extendibility to new software/OS/ DB.	Mean time to repair should be less than 6 hours

Availability	Scalability	Security	Interoperability	Maintenance	Performance	Extendibility	Reliability
Maintenance job should be done between 12 at night to 5 in the morning.		changing the passwords at system-defined intervals.					
The platform features for redundancy/ add -ons for redundancy provided by the system should be enabled.		The system should have strong role based access control logic built in it	The application must allow interoperability with Third party software, COTS, Bespoke Software etc.		All performance related calls from users will be rectified and closed within 3 months		
	The platform should be scalable to serve the increasing number of subscribers.	Compliance to ISO 27001 Standards					

2 Setting up of Infrastructure

- Developing or scaling up the infrastructure such as Data Centre, Disaster Recovery Facility, Network and connectivity, Call Center, Centralized Back Office and any other related infrastructure. The selected applicant should take a sign off on completion of each of the activities from an external professional agency (including the agency utilised for certification of User Acceptance Test (UAT) in terms of this document) having experience in dealing with similar matters. After certification from such an agency that the activity has been completed, the certification along with a declaration from the Chief Executive officer of the applicant on the completion/readiness of the activity needs to be submitted to the Authority.
- Data Migration (Transfer) Strategy and data transfer ensuring System driven coordination of Data.

2.1 Infrastructure Architecture

a) Overview of Infrastructure requirements

The hardware and infrastructure requirements for the solution of CRA with its diverse nature of connectivity and high availability, application should be based on principles of robustness, scalability and availability. Since connectivity would be present with various government agencies, the system needs to be flexible enough to accommodate a diverse nature of network connectivity. The solution proposed needs to be not just failsafe but also scalable and adaptable to the growth in volumes. The successful applicant would be required to provide:

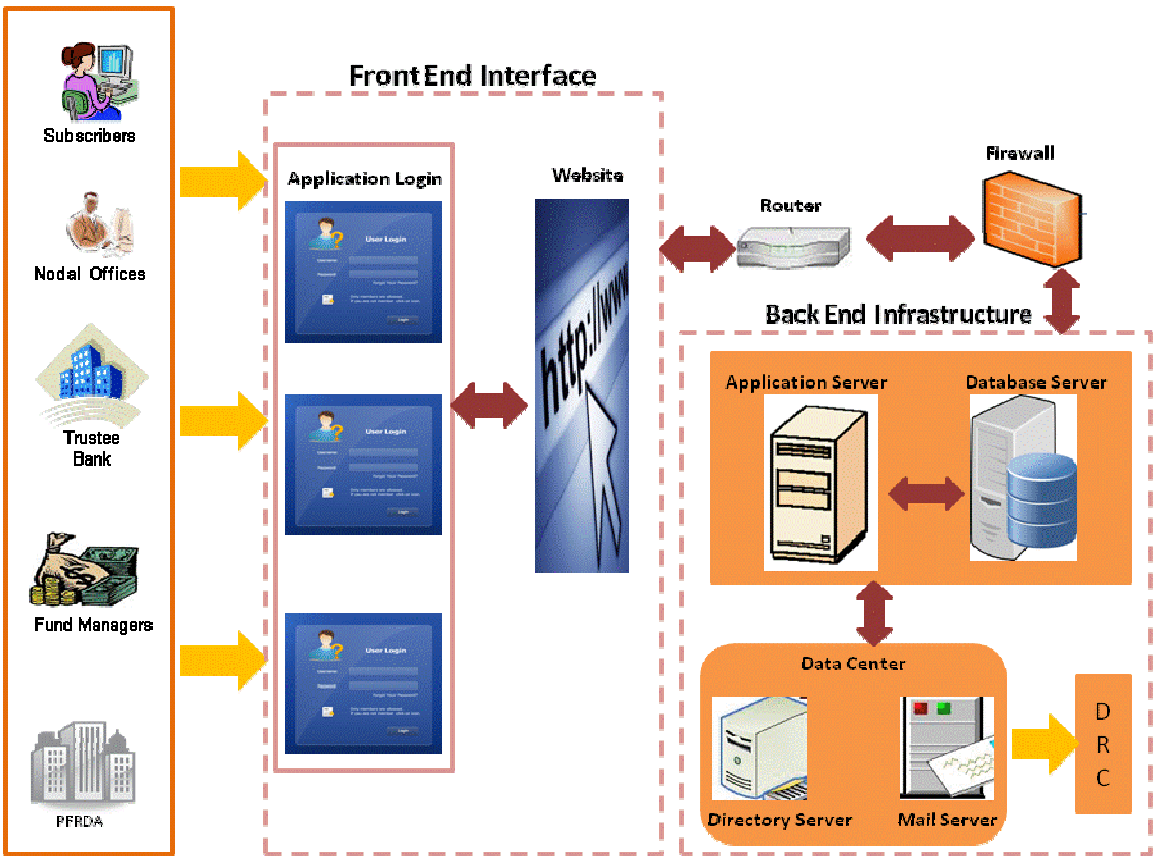
- Data Center
- Disaster Recovery Center
- Network and connectivity
- Call Center

PFRDA provides the liberty to applicants to propose totally new infrastructure or use existing infrastructure with required scaling for the operations relating to CRA. In case the applicant proposes to use an existing infrastructure then segregation, security and integrity of the data must be ensured. In this context the applicant is expected to come up with a detailed strategy highlighting the mechanism to ensure segregation, security and integrity of data.

b) Server Storage Requirements

The infrastructure requirement of CRA system is expected to scale up in the coming years. Inadequate planning and design would result in performance degradation detrimental to the interest of the stakeholders of the CRA system.

To avoid the potential bottleneck the applicant should plan for server storage management in terms of the components required to meet the scalability without compromising on the other parameters. In this regard the applicant is expected to elicit their plan with the server storage architecture to manage server storage without compromising on the performance and other required parameters of the application as specified in the expected performance level table discussed below.



c) Data Center and Disaster Recovery Center Requirements

The infrastructure should consist of amongst other things a Data center and a Disaster Recovery Center, the description of which is given below. This Data Center will form the core of the technical infrastructure. It should incorporate the application components that have been described in the data and application architectures and must be scalable to the needs of growth in terms of user access/transaction volumes/data storage/addition of stakeholders. The functional aspects of the technical infrastructure architecture are given below but the applicant is expected to give the detailed solution. Response expected from applicants with regard to Data Center must include the following:-

- Architecture overview
- Block diagram showing major components of the solution

- Major hardware component features
- Break up of each of the major aspects given as guidelines in this document from implementation perspective

It must be noted that while the application and infrastructure design, development, implementation and operations period are the responsibilities of the CRA. PFRDA has exclusive rights to the entire repository of data.

It is however emphasized that the software and applications must be compatible with the hardware and infrastructure and any issues arising due to incompatibility of the same will have to be resolved by the applicant.

d) Data Center

The Data Center is the central engine on which depends the quality of services to the stakeholders. Its design, implementation and management should be well conceived by the applicant. The data center should provide the following:

- Secure hosting
- Standard technologies
- Guaranteed service levels
- High quality support, operation and monitoring of the application
- Data and Application availability seven days a week, twenty-four hours a day
- Centralized network management and operations capability
- Facility for centralized management of CRA (enterprise client/server) systems
- Custom Security options, Multiple security levels
- Backup, Recovery and Archival Services

e) Data Center guidelines and Data Center Plan

The applicant should ensure that the CRA Data Center facility is secure and exclusively earmarked. In such a case, physical and logical separation (of space and networks) is to be provided to protect CRA data, applications and servers. The applicants have to give a detailed plan as to how they envisage CRA separation requirements providing it with both physical and network exclusivity. A technical audit from the security and controls perspective maybe conducted by PFRDA or through its appointed agency.

f) Other Requirements

Provision of Infrastructure, including:

- Raised Floor
- Electrical Power, UPS and DG backup

- Fire Detection and Suppression
- Humidity, Ventilation and Air Conditioning (HVAC)
- Natural Environment Handling
- Physical Security
- Data/Telecom Cabling

Installation and Integration of the IT Infrastructure, including:

- Servers
- Network active components - switches, routers, passive components - backbone Racks
- Telecom equipment and bandwidth pipes etc
- Enterprise management systems
- Storage primary and secondary
- Security - Firewalls, IDS, IPS, VPNs, Antivirus, Gateway etc
- Security Operation Centre (SOC) and Network Operation Centre (NOC)

g) Space/Rack Requirement

The requirement of rack space should be assessed and proposed by the applicant with a plan to store and maintain master and transaction data.

h) Bandwidth Requirement

The requirement of bandwidth should be assessed and proposed by the applicant in tune with the requirements taking into consideration the various redundancy mechanisms required to maintain service level compliance and uptime needs.

i) Data Center related scope of services

The services required amongst other would fall under the following category:

- Server & application Hosting
- Performance optimization

j) Disaster Recovery Center

The Business Continuity Solution for CRA system should ensure delivery of services to the stakeholders in the event of complete failure of the CRA Data Centre. The DR site must be invoked automatically when the production site fails to provide its services. The applicant is required to submit a detailed architecture and components of the DR solution. DR site shall be setup and maintained by the successful applicant.

The following are the requirements of the DR site

- The DR site should be designed as the backup (mirror) site to the production site.
- The applicant has to offer an optimized, connectivity solution from the CRA application site to the DR Site.
- The DR Site needs to deploy the entire CRA application (1:1) solution.
- The applicant needs to ensure that the DR Site is kept current with the latest version of the application builds, and all solution components.
- The applicant shall simulate routine tests to ensure that the fail-over to the DR Site happens, without any service downtime. The applicant may consider running all services and transactions off the DR Site, at least once in three months, on a non-peak day.
- The applicant will have to perform DR drills every quarter of the year.

k) Backup and recovery

Considering the magnitude of operations and the criticality of the data handled by CRA, it is recommended that a well thought out business continuity plan be put into place. For continuity of operations the applicant needs to propose a solution for a replication site and regular risk assessment strategies. The applicant is required to suggest a solution for the business continuity and disaster recovery aspects of the proposed solution. Some important points amongst other in terms of PFRDA's requirement are as below and are intended as a broad guideline for the solution.

- The applicant should have a documented back up strategy and recovery wherein back up schedules and responsibilities are clearly laid out at an organization level.
- The back-up media should be stored in a secured place and any incidence occurring due to misplacement of media should be immediately reported to PFRDA.
- There should be a regular and updated anti-virus strategy
- All archival media should be stored in suitable facilities and one copy each of media should be stored in fire proof facilities in the premises.
- There should be a copy of media stored outside the premises.
- There should be regularly scheduled restore facilities to test the health of the archive backups and the media.
- Back up log should be maintained for a period of two year.
- PFRDA reserves the right to audit the backup media through an external agency.

- All systems – applications, data tuned parameters and critical hard copy documents would be regularly backed up.

l) Disaster Recovery Plan

- There should be a documented disaster recovery and business recovery plan with regards to its operations.
- The selected applicant must have a replication site at a location not in the physical proximity of the premises.
- The applicant must ensure near real time replication of the transaction data of the live server.
- The replication site should be hosted with the same physical and technical security requirements as the primary sites.
- There should be a documented escalation process and designated personnel who shall be responsible for contact and action in case of disaster.
- There should be routine disaster response drills, the reports of which should be communicated to PFRDA every 3 months.
- All systems should be adequately covered by insurance.
- PFRDA reserves the right to audit the DR site through any external agency.

m) Use of Emerging and Latest Technology: Preferably use of Emerging and Latest Technology Stacks for providing the CRA services with following;

1. Bigdata, Data Analytics, Business Intelligence and Reporting.
2. Cloud Computing.
3. Data Science/AI or Machine Learning.
4. Mobile Applications and Application Program Interfaces (API)
5. Cyber Security and Data Privacy
6. Fin Tech and Sandbox testing enabled solutions to integrate with CRA.

7. Blockchain based smart contracts, record keeping.

8. Integration with Payment Gateways (PG) and Wallets for sharing the data/reports.

9. Integration capability with various Government Systems/Stakeholders Systems as per the requirement of PFRDA in future or time to time.

2.2 Expected Minimum Performance Requirements from Hardware

Availability	Scalability	Security	Interoperability	Maintenance	Performance	Extendibility	Reliability
Should be available for 99.5 % during 8 a.m. to 8 pm and 97.5%from duringthe remaining time.		The system and the DR site should be hosted in a strongly secure physical environment.	The servers should support the proposed application server / database server environment	The applicant should have a qualified maintenance team in place comprising of a network, hardware and platform (OS) expert.	The system response time should be no more than 7 seconds for any query / posting	The system should be extendable to allow addition of storage hardware and external storage devices with least disruption of	The Mean time between failure should be more than 24*30*3 hrs
In case the primary server is down, the secondary server should be able to handle transactions within the next 2-5 minutes. It should support the application till it gets connected to the DR.	It should allow addition of processing units and allow for Clustering of systems.	Compliance with ISO 27001 standards must be ensured		All hardware, platform or networks should be covered under warranty or Service agreements with OEM or their service providers. The initial service agreements should be valid for at least one year from the date of implementation.	There should be performance tuning of the hardware, software and database every 6 months	The system should be extendable to add new service delivery channel eg., mobile phones, PDA etc.	Mean time to repair should be less than 6 hours
The	It should			All performance	There shall be	The system	

hardware architecture should not have single point of failure	allow for storage of hardware and external storage devices with least disruption of services			related calls from users will be rectified and closed within 3 months	at at least concurrent 1500 to 2000 Users logged to the application. Performance must be ensured for	should be extendable to add new stakeholders.	
All routine maintenance downtime should be announced and intimated to the PFRDA at least 120 hours in advance and the maintenance job				Maintenance method should follow some Standard IT Management framework like ITSM.			

2.3 Network Requirement

All the components of the CRA network solution and the application should be designed with resilience to maintain the 24x7 services to all the stakeholders. A checklist of resilient equipment and component should be mentioned by the applicant. It is the responsibility of the applicant to design and deploy a network to ensure 24x7 services of the CRA application. The functional aspects of the technical infrastructure architecture are given below, but the applicant is expected to give the detailed solution. Response expected from applicants with regard to network solution should include the following: -

- Technical overview
- Detailed Network diagram showing major components of the solution
- LAN and WAN components
- Connectivity and technical specifications with regard to connectivity and Perimeter

The network solution may be designed on the scope and guidelines given below

a) Design, installation & commissioning of the LAN and WAN,

b) The scope of work will also include IP addressing, Planning for Redundancy & Security, etc. for various locations of user access as specified by PFRDA.

c) Maintenance of network links between the stakeholders and the CRA's data centre shall be the responsibility of the applicant.

- The bandwidth requirements for meeting the Expected Performance Requirement should be carefully assessed by the applicants.
- The special requirements of the bandwidth at peak-times on peak-dates have to be assessed for performance complying with the Expected Performance Requirements.
- Redundancy in the form of alternative lines of connectivity like leased lines, ISDN, OFC, RF Links etc will have to be provided for.
- An efficient system of monitoring the network performance and availability should be instituted for 24x7 functioning.
- Internet bandwidth requirements at the Data Center will also have to be assessed by the applicants so as to ensure compliance with the expected performance level.

d) All the Networking Elements (Routers, Switches and Firewall) should be from the same or compatible OEM.

e) Local Area Network Connectivity

- The Applicant shall design the complete LAN architecture for the application.

- The Applicant has to plan and design the structured cabling and power cabling and all related works for the successful installation and commissioning of the LAN

f) IP addressing

- The applicant has to design the IP-addressing schemes for the LAN and the WAN
- The applicant needs to design IP addressing keeping in mind the implementation of a Disaster Recovery location also.

g) Network Redundancy and Security

- The applicant must consider in the design that redundancy should be available at all critical points of the network
- The applicant must make sure that all primary links shall be properly backed up as required in the document.
- The successful Applicant shall ensure by proper and careful design of necessary configuration & security policies for the LAN and WAN networks.

h) The successful applicant has to be responsible for provisioning of the required connectivity services for successful and timely implementation between the PFRDA location/s and his premises. He will be responsible for all service-related issues which may arise with the bandwidth provider.

- The successful applicant has to submit all relevant documents pertaining to the entire network, for Remote Management of the Network. This should minimally cover the User Manuals, Operation Manuals, Manufacturer Supplied Technical Documentation, Configuration of all the Network Devices, all relevant diagrams/documentation required in hard copy as well as soft-copy.
- The successful applicant should provide free-of-cost orientation training for two-man weeks to concerned PFRDA officers or its identified personnel in operation, testing, maintenance of hardware and software of the network equipment, interconnection details of attached hardware, general network capabilities and technologies involved and configuration and troubleshooting of the equipment.

2.4 Expected Minimum Performance Requirements from Network

Availability	Scalability	Security	Maintenance	Performance	Extendibility	Reliability
There should be failsafe mechanisms in place for the network and connectivity to the service provider.		Compliance to ISO 27001 standards must be ensured.	The network should be covered under warranty or service agreements with OEM or their service providers. The initial service agreements should be valid for at least one year from the date of implementation.	The network should perform at promised performance levels at any given node of the network.	The network capacity should be extended in not more than 90 man days.	Mean Time Between Failure (MTBF) should be more than 24*30*3
Service availability is the proportion of time the service is fully available to the user. This should not be less than 99.5% during 8 am to 8 pm and 97.5% during the remaining time.		There should be Network security audit at least once in a year	Standard IT management framework like ITSM should be followed.			Meant Time To Repair (MTTR) is the time taken to repair should not be more than 2 hrs from logging of call.

2.5 Call Center

The subscribers of NPS are spread across the length and breadth of the country. In order to provide better service to them PFRDA requires that the CRA should establish an Inbound Call Center with the following service features.

- Separate PRI Line and Toll free numbers for institutions and subscribers.
- Interactive voice response or IVR.
- Hindi / English speaking customer service executives to begin with extend to other languages.
- Scaling up on pro-rata basis to meet the subscriber needs.
- The average wait time for a caller should never exceed 3 minutes.

However, PFRDA may direct CRA on extending further services or scaling up. The Call Center strategy, delineated below, attempts to provide the right kind of services to the subscribers spread across the nation. It should be possible to scale up each component as and when growth in demand occurs. Key requirements from call centre are provided below:

- There should be a response and identification system wherein the caller will be guided through the call login process and send his identification for verification using a unique T Pin.
- It should use the same database and complaint registering software which is used for call logging on the internet.
- There should be provision for operator assistance and call escalation.
- There should be strict adherence to declared service levels and it should be monitored by designated personnel.
- PFRDA reserves the right to appoint an external agency to audit the security and compliance to agreed service levels.

2.6 People Architecture

PFRDA expects the applicant to create a separate unit/entity within existing management structure exclusively for the operations of CRA. The unit would be headed by CRA Head and System Head.

i. CRA Head - The person heading the CRA business should be professionally qualified. The individual should have a proven track record with a demonstrated ability of handling large projects of similar nature. The person concerned will be responsible for the Operations, Systems, Financial, Administration and HR activities of CRA. He / She will directly

report to the MD & the Board of Directors of the organisation and will have no responsibilities other than that of CRA.

ii. System Head - The IT Head of the project should be professionally qualified. The individual should have a proven track record with a demonstrated ability of handling large projects of similar nature. The person concerned will be responsible for the IT & Systems development. He/she will report to the person heading the CRA activities and will have no responsibilities other than that of CRA. IT Head should be supported by Chief Information Security Officer (CISO) – to handle the PFRDA Cyber Resilience Framework related activities as per the PFRDA guidelines as well as the future Information Security related activities. CISO can be shared resource of the group or dedicated as per the convenience of the CRA to provide the support information and cyber security activities.
The overall roles and responsibilities of such a unit would amongst other include:

a) Management of CRA

- To set up the required administrative capacity to meet functional and service obligations of CRA
- Management capacities in execution and overseeing of functions of CRA while meeting expected performance requirements.
- To enforce service and functional guidelines formulated by PFRDA on other stakeholders and report on lapses and errors.
- Formulation of suitable management structure for conduct of business of CRA, with focus on
    - Process improvements and innovation.
    - Solution delivery
    - Service provisioning
    - Strategic planning
    - Enterprise leverage
    - Financial Management
    - Standards and Policies
- Separate structure with specific verticals to focus on service delivery, IT infrastructure and services management, monitoring of service level adherence. This would involve development of separate management unit with clearly defined functions for various

verticals, roles and responsibilities for vertical specific staff. The applicant is expected to provide a detailed description of his approach in creating such unit along with detailed organizational structure. The applicant should also provide details on number of employees to be deployed for various activities and at various levels on both offsite and on site.

- Initiation of service delivery after formulation of detailed business process and workflows as well as quality monitoring systems for measurement of processes and other quality parameters. Applicant should submit complete documentation on workflows to PFRDA before start of implementation. This would require applicant to implement quality improvement/monitoring systems.
- Design of administrative systems based on documents and artifacts supplied, including addressing of all architectural aspects as per the requirements of PFRDA

b) IT management

- Planning for efficient administration of IT, deployment of necessary infrastructure coupled with suitable skilled personnel for undertaking various aspects relating to operations & maintenance and service delivery.
- System for maintaining information security and confidentiality of all records, data and information.
- Formulation of supporting policy/process framework for management of IT. Development of IT governance structure including IT policies and procedures and other polices required for successful conduct of business of CRA. These includes amongst other
  1. IT policy for creation and maintenance of infrastructure
  2. International best practices in IT services management
  3. Information security framework and policy
  4. Quality assurance framework for improvement of overall operations of CRA
  5. Outsourcing policy with respect to processes, people and all related activities of the CRA and which needs to be submitted to PFRDA.
  6. HR policy with HR deployment planning for critical IT operations including backup of suitable man power.
  7. Other policies and procedures for documentation of support function such as accounting and finance etc.

2.7 Expected Minimum Performance Requirements from People Architecture

	Availabilit	Scalability	Security	Manageabilit	Performanc	Reliability
CRA Management	Provide single point of contact on a 24X7 basis	Manpower Planning for meeting the growth	Development & Implement-ation of ISMS	Framework for development and management of IT infrastructure		Plan and deploy Human Resource with their backup plans
			Must ensure data privacy and security	Formulation of business process for service delivery	Adherence to international standards for quality monitoring of service	
			Ensure trained professionals in place for management of security		Adherence to International best practices in IT services management	
Support Staff	Appropriate -ly qualified, trained and experience d people for different verticals	Number of people should be scaled up in accordance with growth	Must sign a contract with CRA in binding to security policy			Plan and deploy Human Resource with their backup plans
IT staff	Appropriatel y qualified, trained and experienced people for different verticals.	Number of people should be scaled up in accordance with growth.	Must sign a contract in CRA for binding to security policy.			Plan and deploy Human Resource with their backup plans.

NOTE: The selected applicant may develop new infrastructure or use/scale-up existing infrastructure ensuring the flexibility of the system to incorporate changes in future in order to meet the changing needs of NPS. In either case, the selected applicant must ensure segregation, security and integrity of pension data. Selected applicant should necessarily meet the Service level parameters.

c) Operation & Maintenance

Subsequent to building infrastructure, selected applicant should operate and maintain the CRA system and provide the services to stakeholders. The applicant should take care of the requirements as given below:

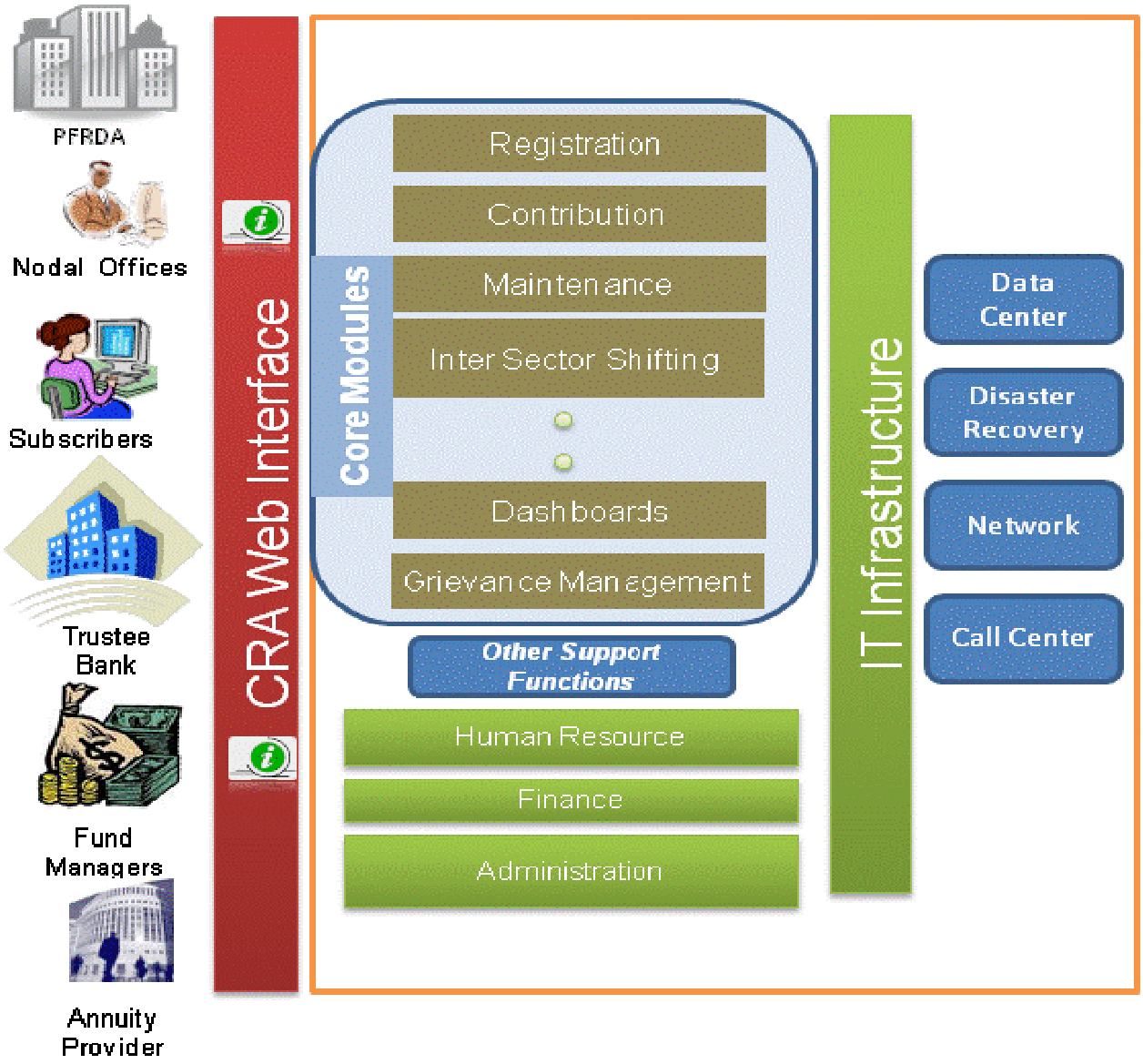
i. Providing services to various stakeholders as per services provided below, while meeting the Expected Performance Requirements or service level parameters (SLs).

ii. Upgrading the applications and infrastructure based on the requirements from PFRDA.

iii. Expanding the operations based on the needs communicated by PFRDA.

3 Scope of work of CRA services

The primary responsibility of designing appropriate solution architecture of the CRA application and providing the services in compliance with the Service Level (SL) parameters rests with the selected applicant.



(CRA Web Interface / CRA Application Program Interface)

3.1 Functional Requirements

Indicative functional requirements of the CRA system are accordingly specified in this section.

- **CRA interfacing requirements:** These requirements primarily arise due to the interfacing requirements associated with the service delivery needs to various stakeholders. The functional architecture should permit transactions of all types to be undertaken by customers and entities such as PRAN account opening, pension fund transfer information, switching investment preference, registering grievances, etc. Stakeholders participating in CRA System should be free from having to design and use disparate systems for their accounting, reporting and MIS requirements. The system should be vastly scalable, secure and reliable and should have the necessary structure for incorporating future requirements associated with service delivery. The CRA system shall be compatible for data sharing or migration or interoperability between the existing CRA system and itself.

- **CRA Activities:** CRA, in order to deliver the services, should take up necessary activities for processing the information obtained from stakeholders. These activities include, but not limited to, consolidated contribution & switching, instruction, PRAN account generation, compile retirement information, trustee account reconciliation, post fund returns. The functional architecture should have the provision for adding any additional stakeholder/instruction into the overall structure as per the requirements of PFRDA.

- **CRA data:** CRA should maintain a repository of data to support interfacing requirements and activities. This includes maintaining amongst other, Subscribers, Accounting, Investment, Pension Contribution, PFMs scheme performance, Trustee Bank communication, Participating States / Organizations / PFMs / Annuity Providers Data.

3.2 Functional Description:

The functional description table provided below lists the indicative key activities associated with each function under CRA

S.No.	Function	Activity	Stakeholder(s)
S.No.	Function	Activity	Stakeholder(s)
1	PRAN Accounts Management	▪ New subscriber registration ▪ Request for issuance of PRAN to CRA ▪ Confirmation Report by CRA ▪ Post PRA Number to Organizations by CRA	Nodal Officers and Subscribers
2	Investment Scheme and Switching	▪ Investment Scheme Selection ▪ Switching over schemes ▪ Confirmation Report by CRA	Nodal Officers and Subscribers
3	Pension Contributions Information	▪ Compile Pension Contribution Information ▪ Matching Contribution Information ▪ Transfer of Contribution Information to CRA ▪ Confirmation Report by CRA	Nodal Officer
4	Trustee Bank	▪ Report of Fund Transferred by Nodal Officer to CRA ▪ Confirmation Report by CRA ▪ Discrepancy Report by CRA ▪ Instruction to Trustee Bank about consolidated investment instruction to PFMs ▪ Instruction by CRA for net fund transfer to PFMs account ▪ Instruction by CRA for fund transfer to Annuity Service Provider. ▪ Instruction to Trustee Bank to transfer fund to Annuity Service Provider ▪ Confirmation Report to CRA	Trustee Bank

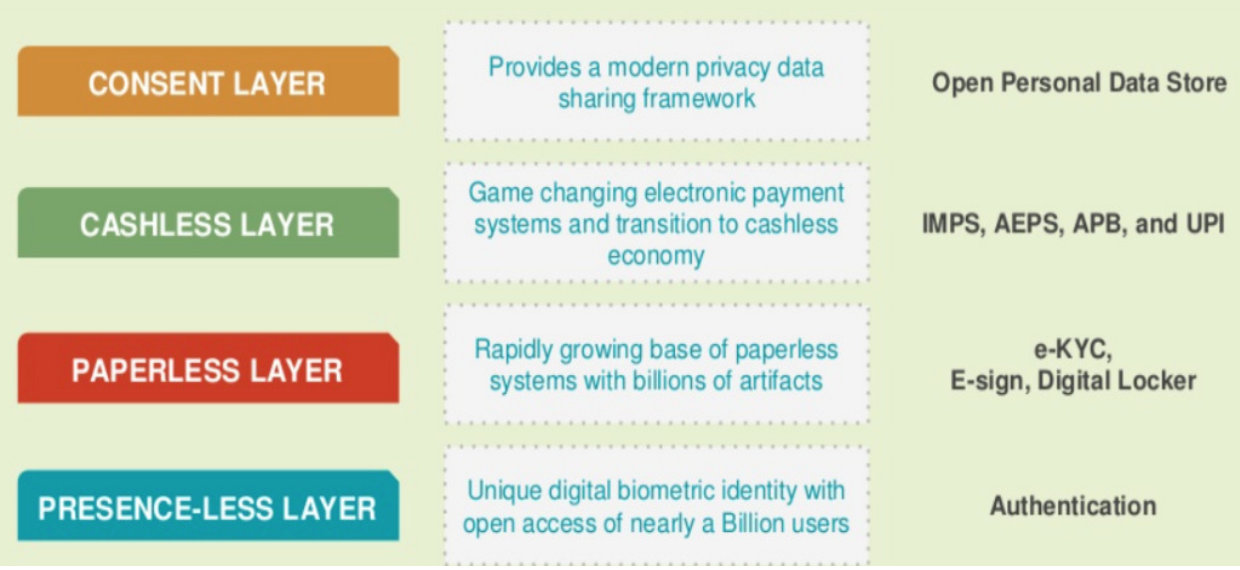
Interfacing requirements, CRA activities and CRA data.

5	PF Communication	▪ Compiled and consolidated investment instruction by CRA ▪ Confirmation Report by PFMs to CRA ▪ Daily investment report by PFMs ▪ Report of scheme wise payout position of PFMs to CRA ▪ Report by PFMs on NAVs of Schemes ▪ Net fund receipt from Trustee Account report by PFMs on different investment schemes	PFMs
6	Annuity Services	▪ List of Annuity Service Providers and Pension Schemes ▪ Selection of Annuity Service Provider ▪ Scheme and investment amount. Detail Pension Scheme Sales Report to CRA	Annuity Service Providers
7	Retirement Information	▪ List of subscribers due to retire within a specified period ▪ Terminal Wealth accumulated in their PRAN ▪ Amount to be withdrawn by subscriber above the mandated limit ▪ Amount to be invested in Annuity	Subscribers
8	View PRAN Account	▪ Personal PRAN Account transaction details	Subscriber
9	Grievance Cell	▪ Registration of Grievance ▪ View Grievance Redressal ▪ Status Report on the grievance ▪ Report on Grievance redressal to PFRDA / Other authority.	Subscriber / PFRDA / Other Authority
10	NPS Data Verification	▪ Verify and Filter NPSCAN data submitted by Government Organizations ▪ Generate Report on data discrepancy ▪ Transfer of Data to CRA System. ▪ Send Report to Organizations, PFRDA.	

S.No.	Function	Activity	Stakeholder(s)
CRA Activities			

1	PRA Number Generation	▪ List of applicants of PRAN Accounts ▪ Validate Investor / Subscriber Information and generate report ▪ Generate PRA Numbers for new subscribers ▪ Transfer PRA Number to Organizations/Departments	Subscriber / Nodal Office
2	Trustee Bank Account Reconciliation	▪ Reconcile organization wise bank account statement with contribution information sent by Nodal officers ▪ Discrepancy Report Generation	Trustee Bank
3	Consolidation of Contributions and switching instructions	▪ Compile and consolidate investment switching preferences and group by scheme and PFMs. ▪ Calculate Amount to be invested in each scheme group by PFMs.	PFM
4	Post Fund Returns	▪ Calculate and post PRAN account wise information. Post periodic statement in PRAN Accounts.	Subscriber
5	Compile Retirement	▪ Generate list of subscriber to retire within a specified period.	Nodal Office
6	Add/Delete State/Organizations /PFMs /ASPs or any other stakeholder	▪ Receive request for enrollment in the NPS System ▪ Validate the credential of the entity ▪ Send report to PFRDA/Other authority ▪ Update and enroll the entity in the NPS System.	Nodal Office

The applicant should assess the requirements of CRA incorporating in it the functional requirements of NPSCAN also. The design and development of the CRA application should be modular in nature so that NPSCAN can be detached from it in a future date. Post detachment both the applications should be able to function as independent applications and also be able to communicate amongst them.



3.3 CRA services common to all the subscribers across various sectors

Please note that the requirements are only indicative and there could be number of other requirements for successful implementation, which may involve system development (NPS, APY, eNPS, Mobile Application) and day to day operational support.

The applicant shall be responsible for delivering services relating to

i. Creation and updation of subscriber Database: Requests from subscriber regarding updation of personal information such as change of address etc. have to be addressed by the CRA system. A confirmation of carrying out the change request would be sent to nodal office and Subscriber simultaneously.

ii. Generation of Unique Permanent Retirement Account Number (PRAN). This service involves:

   a. Application for account opening: The application for opening a PRAN would be filled at the nodal office level by the subscriber and the same duly certified by the department will be sent to CRA. The application would contain the photograph of the subscriber, signature, address and other details.

b. Application processing: The CRA would digitize applications of the subscriber and store it in data base. For this purpose, it is necessary for CRA to setup its own back office with required infrastructure. Generation of PRAN involves creation of Subscriber Information File (SIF). After examining details for minimum information requirements, CRA would store subscriber information record. After creation of the subscriber's information record in database, a unique PRA number will be generated automatically. *The PRA Number, as per the requirements of PFRDA, should be printed on a plastic card along with photograph and signature of the subscriber*.

c. Issuance: The PRAN card along with other information through an NPS kit (information on PFMs, Schemes, Grievance escalation procedure, contact information, frequency of switching etc.) should be sent to departments. Subsequently, the cards will be handed over by departments to the respective subscribers. I-PIN and T-PIN should be provided to all the subscribers within ten days of opening of PRAN account.

iii. Consolidation of Pension Contributions Information

iv. Consolidation and grouping of investment preference on the basis of schemes and PFMs

v. Sending Annual Account statements: Periodic PRAN account statements should be sent to subscribers/investors detailing the total contribution, time-wise credits into the account and other relevant information. The statements shall be made available in regional languages also and as per the directions of the Authority.

vi. Grievance redressal report: Subscriber should be able to register grievances through the web interface. Alternatively, subscriber should be able to send grievances through other channels also. However, CRA should register all complaints in electronic form. The status of grievance / redressal should be sent to subscriber.

vii. Web enabled services: CRA should provide subscribers with a web based interface to view detailed history of transactions of PRA lodge and check Withdrawal Claim and select the ASP and the Annuity Scheme.

viii. In due course subscriber should be able to give switching instructions through this interface. The scaling up (in view of increase in transactions or subscribers) and up-gradation of system (in view of new technologies) would be the responsibility of the applicant.

ix. Generate reports on errors and discrepancies on NPSCAN data: Any errors in the NPSCAN data would be immediately intimated to Government Department/NPSCAN. Departments would access this information for making necessary corrections. CRA application should be designed to trace such mistakes.

x. Creation of a dedicated NPS withdrawal Claims Processing Cell for receiving, processing and settlement of all withdrawal claims under Tier I and Tier II accounts of NPS in accordance with the rules, regulations and guidelines of PFRDA and related functionalities. The work entails both online as well as manual processing of the withdrawal claims depending on the nature of the withdrawal reported and in accordance with the instructions in this regard from NPS Trust. This includes development of IT interface for processing the claims online and offline and interface with Annuity Service Providers systems for selection of Annuity service provider and purchase of annuities by subscribers of all sectors. The NPS withdrawal claims process shall be in accordance with PFRDA (Central Recordkeeping Agency) Regulations, 2015 and amendments thereunder and PFRDA (Exits and Withdrawals under NPS) Regulations, 2015 and amendments thereunder. In case of any ambiguity, the decision of PFRDA is final in this regard.

xi. a) Grievance by subscribers: Consolidate grievance and complaints of subscribers and corresponding service providers: Subscriber would be provided with facility to express grievance through IT platform/non-IT platform whereby subscribers/nodal offices would access the web site of CRA to register their grievances. In case of unavailability of access to internet, the subscriber would manually submit his/her grievance to Nodal office or directly to CRA. Upon receiving the grievance, respective Nodal office, would record this grievance into the web based interface provided to him. Alternatively, if the grievance is sent to the CRA manually, then the “Centralized Back Office” shall immediately make the entry in the CRA application. The web based interface should support in registering several types of grievances. Depending on the type of grievance, further escalation should take place automatically. Hence, CRA application should support the grievance redressal process by providing necessary web interface to support grievance recording operations of nodal office. However, a report on the status of grievance registration including number of complaints received category wise etc. should be generated by CRA for the purpose of monitoring by PFRDA. Registration and resolution of grievances shall be in accordance with PFRDA (Redressal of Subscriber Grievance) Regulations, 2015 and amendments thereunder.

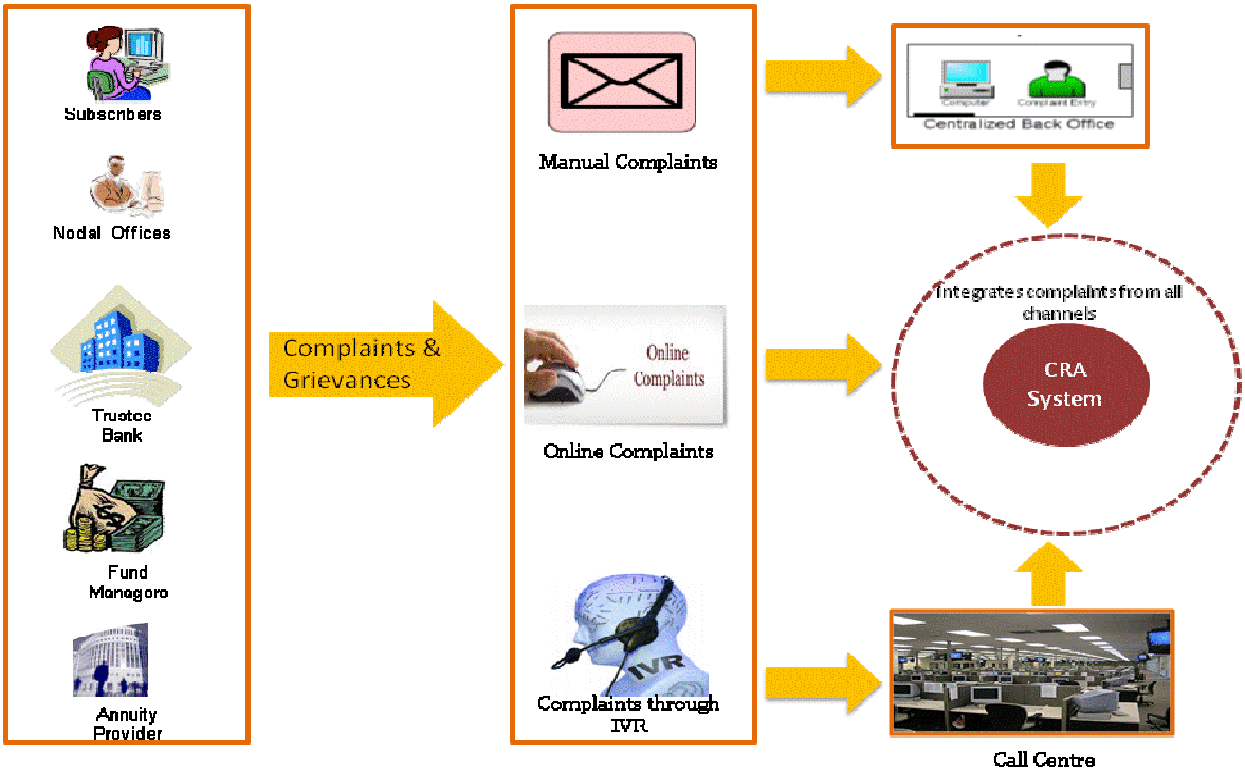
b) Grievance by Nodal offices: The web based interface should have the required facility to capture grievances of Nodal offices and the departments concerned. The facility should include registration of grievances against other entities such as PFMs and CRA. A grievance and redressal status of the complaint needs to be updated and an MIS report should be generated as per the requirements of PFRDA. This report should be sent to the concerned parties. An escalation mechanism would have to be built into this to ensure fast grievance redressal.

c) An indicative grievance and complaint workflow is provided below

1) Complaints can be registered by subscribers in either of the mechanisms viz., manual i.e., by post or courier, through service center (Telephone) or through CRA web interface. In case of complaint received through letter, the CRA back office should enter the details in the application and intimation should be sent to the aggrieved subscriber.

2) In case of manual complaint there will be a standard form for registration of complaints which should be available in all the government offices. The form shall be provided by CRA to the government departments. Subscriber will fill the application, and send it by post/courier to the CRA along with the supporting documents.

3) Similarly, complaints registered through the service center would be entered in the application and intimation given to the subscriber on a real time basis. Complaints can be registered through the web interface. In all the cases, a unique grievance number should be generated for tracking the status of complaint resolution. In a similar fashion, other entities can register their complaints. Data from these sources are to be processed and sent to the concerned entity through the web interface.



xii. Prepare Action Taken Report on the grievance and complaints of the subscriber/ investor: An action taken report will have to be submitted to the concerned department on the status of redressal and the number of complaints pending and other relevant information as required by PFRDA.

3.4 Providing various services to all the stakeholders of NPS

This section indicates the services currently identified for the CRA. CRA is expected to incorporate changes as may be indicated from time to time by PFRDA.

3.4.1 Services from CRA to Trustee Accounts

i. Receive reports on investments made by each PFM in different schemes and send instruction to Trustee Bank to remit amount for clearing

ii. Reconcile pension fund reports received from Trustee Account with pension fund contribution information report

iii. Generate error/discrepancy report on fund reconciliation: CRA would generate a funds reconciliation report, after obtaining funds transferred report from Trustee Bank. An arrangement should be made to receive information from Trustee Bank in an electronic format. Reconciliation would involve reconciliation of information on funds credited to each subscriber's PRAN account vis-à-vis amount credited to Trustee Bank. The information on instructions and funds will

be initially stored in NPSCAN. Upon successful reconciliation, filtered data from NPSCAN will be transferred to CRA data base. However, the error/exception/discrepancy reports on reconciliation will be generated instantaneously and will be sent to respective departments. Methodology for corrections to be performed on NPSCAN will have to follow standard accounting principles such as reverse entry etc.

iv. Sending instruction to Trustee Bank to remit withdrawal fund to subscribers' account and remit remaining amount to Annuity Service Providers' account against the annuity scheme

v. Pension fund contribution/collection report: CRA has to provide a facility to receive aggregate and detailed report of funds credited to Trustee Bank on behalf of various sources.

vi. Generate error/discrepancy report on fund reconciliation: Error/discrepancy report will be generated based on reconciliation of funds and a report will be sent to Trustee Bank on a daily basis.

vii. Funds transfer report: CRA will create a facility where Trustee Bank should be able to send a report on daily basis about funds transferred to Pension Fund Schemes Account for settlement of pension fund investments.

viii. Retirement funds transfer report: CRA will create a facility for Trustee Bank to send report on amounts transferred to ASPs and superannuated subscribers. A reconciliation process should be executed subsequently.

3.4.2 Services from CRA to Pension Fund Managers (PFMs)

i. Preparation and sending of consolidated Investment Preference Scheme information: CRA would consolidate (on the basis of scheme and preferred PFMs) investment preferences of subscribers and send this information to PFMs as specified in the Service Level Parameters.

ii. Provision for sending net payout report: The CRA would create a facility to receive net payout report of daily market sell/buyout send by PFMs to CRA.

iii. Discrepancy/confirmation report on net payout: The CRA would create a facility to receive discrepancy report on PFMs net payout status. Any discrepancy/errors/mismatch would be reported to PFRDA immediately.

iv. Funds transfer Report: The CRA should send net fund transfer report to PFMs, on the basis of confirmation of fund transfer report received from Trustee bank.

v. Scheme performance reports: The CRA would create a facility for receiving the daily performance reports of the schemes measured using NAVs send by PFMs to CRA. The interface provided to PFMs should be able to capture this information in the required format.

3.4.3 Services from CRA to Nodal offices / PFRDA / NPS TRUST

Various types of **MIS/Pension Data Analytics** reports should be generated by CRA Using best of the Data Science/AI based or any other latest tools, these include:

i. Number of PRAN issued on a daily basis and PRAN request pending
ii. Funds deposited with Trustee bank
iii. Error/discrepancy/exception reports on NPSCAN/PFMs/Trustee bank
iv. Scheme preferences report
v. Monthly/quarterly/ periodic reports
vi. Service Level parameter(SL) compliance reports (service levels and IT infrastructure performance SL's)
vii. Status of Complaints(Nodal offices/PoPs/Aggregators)
viii. Complaints resolution status reports
ix. Performance report of PFMs, Nodal offices, PoPs, Aggregators.
x. Supervisory and Regulatory Compliance Reports on PFMs and Annuity Service Providers and other stakeholders
xi. Report on errors, lapses and discrepancies of PFMs, Nodal offices, PoPs, Aggregators.
xii. Any other reports as required by PFRDA.

Generation of these reports should be automatic & system driven with least manual intervention. The application so designed should provide a view for Departments/PFRDA to access the reports automatically. In addition, application should also provide the necessary functionality for generation of queries on variety information contained in CRA database. The query results should be exportable to desired formats as per the requirements of PFRDA. PFRDA should be able to demand any other information/clarification required thereof through the interface. The clarifications sought should be stored for record purposes.

3.4.4 Services from CRA to Annuity Service Provider

i. Collection of physical application forms from the subscribers and forwarding them to ASP.

ii. Funds transfer details for the subscriber's annuity to ASPs.

iii. Electronic data transfer to ASPs with respect to subscriber details.

iv. Sending instruction on Annuity scheme: Annuity Service Provider would be provided with a web based interface detailing the annuity scheme and subscriber details for prospective sale.

v. Confirmation on sale of annuity scheme: Annuity Service Provider should be able to send confirmation report of sale of annuity scheme to superannuated subscribers.

vi. Grievance and redressal: The web based interface should have the facility to capture grievances of Annuity provider. A grievance and redressal status of the complaint needs to be updated in the system and MIS reports should be generated as agreed and sent to the concerned parties.

vii. Confirmation of fund transfer from Trustee Bank: Web based interface should have the facility to update information relating to receipt of funds transferred by the Trustee Bank.

3.4.5 EXPECTED MINIMUM LIMIT FOR PERFORMANCE REQUIREMENTS IN DELIVERING SERVICES

Services from CRA	Availability	Scalability	Manageability	Performance	Extendibility	Reliability
NPSCAN						
Generation of PRA Number and Issuance	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time		Manage the system with providing for appropriate support taking into consideration the expected scalability	Till date of dispatch of PRAN Card within 15 days of successful submission of application.		99.9%
Error/discrepancy reports on CRA website	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time			End of the day		99.9 %
Grievance and complaint registration	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time			Instant in case of electronic and IVR complaints. Within 3 days in case of manual complaint		99.8%
Update Subscriber information	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time			Within 2 days		99.8%
Generate	99.5%		Minimum 5 lakhs			99.9%

Services from CRA	Availability	Scalability	Manageability	Performance	Extendibility	Reliability
error/discrepancy report on fund reconciliation	between 8:00 AM - 8:00 PM 97.5% for the remaining time		record from the beginning			
PFM						
Scheme performance reports	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time		Should comply with the increase in number of schemes	End of Day	Should comply with increase in number of schemes	99.9%
Provision for sending net payout report	99.5% between 8:00 AM - 8:00 PM 97.5% for the remaining time		Should comply with the increase in number of schemes	End of Day		99.9%
Discrepancy/confirmation report on net payout	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%		Should comply with the increase in number of schemes	End of Day		99.9%
Funds transfer Report	99.5% between 8:00 AM - 8:00 PM,			End of Day		99.8%

Services from CRA	Availability	Scalability	Manageability	Performance	Extendibility	Reliability
	after 8:00 PM 97.5%					
Trustee Bank						
Pension Fund contribution/ collection report	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%					99.8%
Retirement Funds Transfer Report	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%			End of Day		
Services from CRA to PFRDA/GoI/DEA	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%					99.8%
Annuity Service Provider						
Sending instruction on Annuity scheme	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%					**99.8%**
Confirmation on sale of annuity scheme	99.5% between 8:00 AM -					99.8%

Services from CRA	Availability	Scalability	Manageability	Performance	Extendibility	Reliability
	8:00 PM, after 8:00 PM 97.5%					
Grievance and redressal	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%			Within 5 days of registration of complain		99.8%
Subscriber						
Sending Periodic Account statements				6 months	30%	99.8%
Grievance redressal report	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%			Within 5 days of registration of the complaint		99.8%
Web enabled services	99.5% between 8:00 AM - 8:00 PM, after 8:00 PM 97.5%					99.8%

4. Service Level Requirements

The following table provides the details of the expected minimum service levels from CRA in course of developing application and infrastructure. The applicant should adhere to the timelines strictly and this section provides service level agreements during building infrastructure and operations for service delivery.

4.1 Service Level Parameters for Building Infrastructure

Applicant is expected to adhere to the timelines in building infrastructure as provided in project schedule.

Non-adherence to the time lines in regard to the deliverables would result in payment of compensation and as notified by the Authority. However, the compensation for delays during the building of CRA infrastructure will be decided by PFRDA in discussion with the successful applicant.

4.2 Expected /permitted maximum time limit for Service Level Parameters for Operations and Maintenance

S.No.	Service Matrix Parameters	Base line	Breach	Basis of Measurement
		Metric	Metric	
1. Services and Operations Related				
1	Error/discrepancy reports	End of the day	After 1 day	NA
2	Registration of Grievance and Complaint of subscribers	1-2 days	> 2 days	Measured from the time complaint / grievance received.
3	Action Taken Report on grievance and complaint by subscriber.	Up to 5 days	> 5 days	Measured from the day of registration
4	Action Taken Report on Grievance by Nodal offices	Up to 5 days	> 5 days	Measured from the day of registration
5	Generate PRA Number and send to concerned nodal office (including generation of plastic PRAN card with photograph and signature)	Up to 10 days	> 10 days	Measured from the day of receiving of application to the day
6	Update subscriber's personal information	Up to 2 days	> 2 Days	NA

S.No.	Service Matrix Parameters	Base line	Breach	Basis of Measurement
		Metric	Metric	
	To PFM			
7	Preparation and sending of consolidated Investment Preference Scheme information	End of the day	After 1 day	Measured from the time of receipt of report from Trustee Bank
8	Discrepancy/confirmation report on Net Payout	Up to 2 hrs	> 2 hrs	Measured from the time of receipt of Net Payout Report from PF
9	Funds Transfer Report	Up to 2 hrs	> 2 Hrs.	Measured from the time of confirmation of Net Payout report
10	NAV Report of scheme	End of the day	Not uploaded by EOD	NA
	To Trustee Bank			
11	Generate error/discrepancy report on fund reconciliation	2-3 hours	> 3 Hours	Measured from time of receipt of Trustee Bank report
	To Subscriber/Voluntary Investor			
12	Send Periodic Account statements.(UPC)	2 months	>2 months	Measured from the end of the period for which account statement is required to be sent
13	Grievance redressal report(UPC)(Non-IT based)	Up to 7 days	> 7 days	Measured from the time complaint / grievance received.
14	Processing of Exit and Withdrawal request of the subscribers and issuance of withdrawal and redemption instruction by the CRA (subject to claim being in order)	Up to 7 days	> 7 days	Measured from the time Exit / Withdrawal claim is received by CRA.
Note: PFRDA reserves the right to revise the above timelines based on emerging experience in consultation with stakeholders and introduce any other new parameters for improving/protecting the subscribers' interest.				

4.3 Compensation in case of breach of Service Level Parameters:

Applicant is expected to strictly adhere to Service Level parameters and expected performance requirements provided above, failing which, would result in imposition of compensation/damages. The set of compensation/damages that the CRA shall be liable for such breaches shall be notified by the Authority from time to time by way of circulars.

5. Deliverables and Project Schedule

PFRDA will register the successful applicant as a CRA for setting up of CRA infrastructure. The successful applicant would initiate the necessary studies required for developing infrastructure, application and for conducting data migration and other required studies.

5.1 Deliverables

The deliverables of the project would be as follows:

- Detailed Project Plan and Schedule.
- System Requirement Specification Report.
- System Analysis Design Report including ER diagram and User Interfaces.
- Solution Architectures viz., Logical and Functional Architecture including module description.
- Data Center and Disaster Recovery Center Design Network Design
- Setting up of Data Center, Disaster Recovery Center.
- Setting up of Network, Security Operation Centre (SOC) and Connectivity.
- Application and Mobile App with source codes in two sets, along with source code of third party API/COTS/Bespoke software or any other software used.
- Interoperability – Data Migration Strategy Report
- Interoperability - Data Migration
- Orientation training to all Stakeholders under NPS

Documents to be provided

- User Manual of the application
- Technical Manual of the Application, Data Center, Data Recovery Center and Network
- Training Manual of CRA Application

Project Status Reports - weekly progress reports summarizing

- Results accomplished during each week
- Cumulative deviations to date from schedule of progress on activities
- Corrective actions to be taken to return to planned schedule of progress

- Proposed revisions to planned schedule
- Other issues and outstanding problems and actions proposed to be taken

5.2 Training to Key Staff of NPS Trust, Nodal offices & PFRDA

Applicant in consultation with PFRDA shall develop a detailed orientation training plan for training all stakeholders under NPS including the Government departments. This training would be an executive training, focusing on details of training of officials of stakeholders and Government departments in using CRA/NPSCAN application for generating various reports for monitoring and regulatory purposes. Applicant is also required to submit User Manuals as per the requirements of PFRDA. This shall include training to all the intermediaries registered with PFRDA as is advised by the Authority.

5.3 User Acceptance Test

The selected applicant shall get the User Acceptance Test (UAT) of the CRA system done by an independent specialist firm which has experience in dealing with conducting and reporting on such user acceptance tests as soon as the applicant declares the system to be ready for the exercise. Such a firm proposed for conducting the user acceptance test shall be finalized in consultation with the Authority. However, the Authority reserves the right to engage the services of an external agency to test the CRA system. Any bugs identified during the UAT should be fixed by the implementation applicant before acceptance of the software by PFRDA.

The primary goal of Testing & Acceptance would be to ensure infrastructure developed by applicant meets requirements, standards, specifications and performance prescribed for ensuring that the following are associated with clear, quantifiable metrics for accountability:

a. Functional Requirements
b. Availability
c. Performance
d. Security
e. Manageability

The project is to be designed to meet all functional, non-functional and management requirements.

Functional Requirements

Indicative functional requirement of CRA system is provided together with respective deliverables and a set of standards, wherever applicable. The applicant shall conduct a detailed SRS and submit to PFRDA before implementation for their comments, and based on it, shall develop the CRA system.

Performance

1. Performance is that aspect of service, which is measured in terms of throughput and latency. Higher throughput and lower latency values represent good performance of a service. Throughput represents the number of service requests served. Latency is the round-trip time between sending a request and receiving the response.

2. This test process will include the following activities:
    a. Determination of performance metrics
    b. Designing performance tests
    c. Development of workload
    d. Performance testing
    e. Identification of bottlenecks and providing solutions
    f. Determining final performance figures.
    g. Communication of final results to all stakeholders

3. Final output of this process would be a sizing guide for the solution tested. The sizing guide will document the details of the performance tests, test data, bottlenecks identified, and the final performance data.

Availability

1. High availability is a key requirement. The project must provide subscribers with timely, continuous access to information. The project must also be able to rebound or recover from any planned or unplanned system downtime, ensuring a minimal impact on the operations.
2. Availability is the quality aspect of whether the service is present or ready for immediate use. Availability represents the probability that a service is available. Larger values represent that the service is always ready to use while smaller values indicate unpredictability of whether the service will be available at a particular time.
3. Also associated with availability is time-to-repair (TTR). TTR represents the time it takes to repair a service that has failed. Ideally smaller values of TTR are desirable.
4. The availability test would include the following activities
    a. Designing test for high availability testing
    b. Execution of high-availability tests
    c. Assessment of transaction/data losses in relation to Disaster Recovery system
    d. Communication of final results to all stakeholders

Security

1. Security is the aspect of the service of providing confidentiality and non-repudiation by authenticating the parties involved, encrypting messages, and providing access control. The applications can have different approaches and levels of providing security, depending on the service requester.
2. Security process will include:
    a. Audit of Network, Server and Application security mechanisms
    b. Assessment of authentication mechanism provided in the application / components / modules
    c. Assessment of data encryption and privacy mechanism
    d. Assessment of data access privileges, retention periods and archival mechanisms Final outcome of this process would be a comprehensive audit report including all the Network, Server and application security features incorporated in the CRA system.

3. Register with NCIIPC as Critical Information Infrastructure as per the PFRDA Cyber Resilience Framework guidelines.
4. Data Centre should be Tier 3 and ISO 27001 and related Certification.

Manageability

Manageability needs to be a crucial aspect of an Enterprise Solution. Applicant has to ensure that the solution deployed has adequate monitoring and tracking features for measuring the utilization and availability of resources. This includes:

1. Remote monitoring of Status and Statistics of all high-level components
2. Management capability to start/stop/restart services and systems
3. Auto discovery of all components manageable
4. Auto discovery of all other system components
5. Ability to track changes in configuration of the system components to help track service
6. System disruptions

5.4 Project Schedule

S.No	Activities	Time for Completion*
1)	Acceptance of application of the successful applicant	Date of Start (T)
2)	System Requirements Specification Report, including: ▪ ER Diagram ▪ System Analysis and Design	T + 6 Weeks
3)	Solution Architecture and Design, including: ▪ Logical & Functional Architecture including the application modules	T + 8 weeks
4)	▪ Network Design ▪ Data Center and Disaster Recovery Center Design (DC/DRF) ▪ Server Storage Management Architecture	T + 12 Weeks
5)	Development of CRA Application	T + 24 Weeks
6)	Infrastructure set-up completion, including ▪ DC/DRF ▪ Network and Connectivity ▪ Call Center	T + 28 Weeks
7)	Development of Data Migration Strategy and migration of validated data	T + 30 Weeks
8)	Training to key staff	T + 32 Weeks
9)	User Acceptance Testing	T + 34 Weeks
10)	System ready for “Go-Live”	T + 38 Weeks

*Inter–se changes amongst activities can be discussed with the successful applicant within the project completion period. These timelines are indicative.

6. Technical Proposal Format

The Technical proposal should address the following strictly in the order given below:

1. Understanding of the CRA and National Pension System objectives
2. Approach for setting up the CRA
    a. Overview of the proposed solution that meets the requirements specified
    b. Strategy for setting up of CRA

3. Implementation methodology, project plan and implementation schedule covering all activities, milestones and timelines.

3. Operational methodology
4. Interoperability features (with existing CRA)

5. Proposed architectures
    a. Overall Architecture
    b. Technical Architecture
    c. Security Architecture
    d. Network Architecture
    e. Data Center and Disaster Recovery Center architecture

The applicant shall provide details of its plan to address the technology requirements, such as scalability, availability, performance requirements of the system mentioned.

6. Business plan including
    a. Operations and Maintenance Plan
    b. Human Resource Plan including outsourcing policy related to all the activities of the CRA
    c. Financial Plan
    d. Plan for other support activities

7. Manpower deployment plan
    a. Project team structure, size and capabilities
    b. A specific description of prior experience and expertise of the resources to be dedicated for the project.
    c. Resumes of CRA Head, System Head and key manager(s) are responsible for the management of the project and team, highlighting relevant experiences.
    d. Resumes of the personnel who would be directly assigned/responsible to provide the major services/functions as pertains to the operation of CRA and the specific function each individual would perform.

7. Innovative suggestions that the applicant may want to render w.r.t. the approach adopted for the assignment in the light of their expertise or experience from similar assignments specifically
   a. For service delivery improvement and
   b. Data synchronization between two CRA systems
   .
8. Bill of Material of all components proposed for solution (e.g. software, hardware etc.).

9. Track Record & Experience with similar activities.
   a. Experience in creating, maintaining technology based Centralized Recordkeeping and Management System
   b. Experience in building and maintaining Data Centre & Disaster Recovery Facility
   c. Experience and ability to electronically link with a secure, widespread network of locations with adequate redundancies to ensure uptime in excess of 99%
   d. IT standards and policies followed by the organization
   e. Experience and ability to manage an IT based accounting system that centralizes the settlement of various security transactions

(Brief write-up (Not more than 3 Pages) on relevant experience along with client details for whom mentioned activities have been carried out. Also provide Citation as per Annexure VII)

10. Years of experience in creating, maintaining technology based Centralized Recordkeeping and Management System

(Provide relevant Citation as per Annexure VII (clearly indicating Years of Experience)

11. Number of accounts/subscribers handled each year in the last three years

(Provide Year wise Number of Accounts handled in last three years (Details to be signed by Authorized Signatory)

12. Experience and ability of the entity to manage and run IT based applications in financial domain. (Provide relevant Citation as per Annexure VII (clearly indicating Client details and its areas of operation)

13. Quality assurance/process

14. Key Deliverables (along with example deliverables, where possible)

15. Deviations and Exclusions: The applicant shall provide the deviations and exclusions, if any, from the defined scope of work
16. Applicant Undertakings: Applicant's guarantee for accomplishing the implementation schedules for completion of key deliverables.

17. Total Responsibility: Applicant should issue a statement undertaking total responsibility for the defect free operation of the CRA solution.

18. Any other information that applicant thinks would be worth mentioning in the proposal.

7. Site Visit by PFRDA

As part of the evaluation process, PFRDA and / or any agency selected by PFRDA shall be allowed to visit and examine/verify the applicant's system capabilities as defined in the Technical Proposal. The applicant, if asked by PFRDA, shall arrange and facilitate such visit. The cost of such visits to the sites shall be at PFRDA's expense.

8. Rights over the Work Products/Deliverables & Confidentiality

The ownership including intellectual property rights over all work products/deliverables/data and other intermediate documents generated by CRA under and in relation to the work undertaken by it under the contract shall vest with PFRDA. Further all the documents submitted by the applicant along with the bid or during the course of the presentation shall be exclusive property of PFRDA and shall not be returned back to the applicant.

CRA shall not disclose any part of the information acquired during the course of its working to third parties and shall maintain strict confidentiality, except to other intermediaries, under the NPS Architecture, as is necessary for the discharge of its functions under the contract, failing which it shall be held liable.

Other point which may be included –

1. **Requirement of NPSCAN/Accounting network to initiate/pass instructions to intermediaries. :** NPSCAN shall be a web based 'NPS Contribution Accounting Network' to be developed by the CRA to maintain accounts of Government subscribers. PAOs access NPSCAN for uploading subscriber contribution file, updating various types of request of subscribers such as change in subscriber details, change in scheme preference, switch, withdrawal etc. From technical perspective, all Government transactions are recorded/requested on NPSCAN and then replicated (almost real time) on CRA system, for execution of those transactions.

2. Format for proposed solution for meeting expected Service Delivery

The applicant is expected to explain the methodology through which he will address the technical requirements to meet the expected performance requirements as specified in the tables of RFP. The applicant shall list down the sub requirement within each parameter depicted in the left vertical pane of the following table (Technical Evaluation Framework) against each technology component. In the Reference column the applicant shall give a reference (page no.) to the place in the proposal where he has dealt with that issue.

The applicant may use one architecture diagram to address more than one evaluation parameters **Technical Evaluation Framework**

Parameter/ Technology	Hardware	Application and Platform	Network	Reference Hardware	Reference Application and Platform	Reference Network
Availability						
Scalability						
Security						
Interoperability						
Manageability						
Performance						
Low Cost of Ownership						
Extendibility						
Reliability						

9. This issues with the approval of Competent Authority.

(General Manager)
Regulation Department-CRA