Office of the Comptroller General of India

Request for Proposal for IAAD Centralised Pension Processing Project

Notice for Inviting Comments on Draft RFP Document (Part -2)

Ref: IAAD/CPP/RFP/Notice/03

28 July 2021

Dear Prospective Bidders,

The Indian Audit & Accounts Department under the Comptroller & Auditor General of India (C&AG) is envisaging design and development of a centralized IT Application for facilitating processing of pension of state government employees across 19 states in India. In this regard, IAAD conducted a workshop for prospective solution providers on March 11, 2021.

The Department is currently in process of finalizing Request for Proposal (RFP) document for this Project. The RFP consists of three volumes – Volume I: Functional, Technical, Operational and Other Requirements (supported by Annexures – A, B, C and D), Volume II: Commercial and Bidding Terms and Volume III: Master Service Agreement (supported by Annexure A).

In our endeavor to seek comments/ suggestions from prospective System Integrators, the department has publicly shared first part of draft RFP (Vol- I, Vol – III and Annexure -A to Vol -III) *vide* notice IAAD/CPP/RFP/Notice/02 dated 10.06.2021. Now the following parts of draft RFP are being published for comments:

1. RFP Vol I - Annexure B (Technical Architecture Requirements)
2. RFP Vol I - Annexure C (Technical Specifications & Compliance Requirements)

The remaining parts of the RFP draft would follow.

Comments/suggestions may be sent to cppproject@cag.gov.in by 11 August 2021.

RAGHVENDRA SINGH

Digitally signed by RAGHVENDRA SINGH
Date: 2021.07.28 17:29:14 +05'30'

(Raghvendra Singh)
Director (IS)
O/o the C&AG of India

2021

Request for Proposal

Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

"Centralized Pension Processing System (CPP project)"

Volume – I

Annexure B

Technical Architecture Requirements

Contents

1 Introduction

This document provides envisaged indicative Architecture for CPP solution inclusive of Functional, Information, Application, Technical, and Security Architectures and all related technical aspects. Objective of this document is to provide guidelines, adherence to standards and benchmark SLA as applicable.

1.1 General Guidelines

Bidders should follow the following general guidelines while architecting and designing for CPP solution:

1. **Adapting to evolving technology**: It is preferable that the system is built on open Source, open standards, and open Architecture. System should have a modular approach, with loosely coupled modules, so that changes can be made in modules/ sub-modules without affecting other parts.
2. **Cloud based architecture:** IA&AD mandates the CPP solution to be hosted on MeiTY empanelled Cloud. The architecture should try to maximise the benefit offered by Cloud based solutions, in terms of scalability, agility, inter-operability and less upfront cost. IA&AD shall prefer PaaS ("Platform as a service") model over other models of provisioning the various Network, Infrastructure and Security components on VPC.
3. **High availability:** The entire CPP solution should provide high availability for all components associated with it within the Primary Datacentre (DC-1) as well as the Secondary Datacentre (DC-2).
4. **Single Cloud Service Provider (CSP):** The entire CPP solution (including its Disaster Recovery setup) shall be setup on a single CSP. Hosting of different services/components on multiple CSPs is not permitted. However, backup/archived data/files must be kept at a distance of atleast 300 kms from either DC-1 or DC-2 even if it warrants engagement of a different CSP.
5. **Seamless integration:** The CPP solution is intended to integrate with HRMS and IFMS systems of various state governments (through an API, MFTP based interfaces, etc.) to receive data for processing. Similarly, various outputs of CPP should be shareable with third party services like IFMS, Digi-locker, Treasury, banks etc.
6. **No vendor Lock-in:** Bidders should be able to demonstrate that the components proposed as part of the architecture will not result in a vendor or product lock in situation.
7. **Web-first design:** The CPP Applications should be provided as a web-based solution that should follow a responsive web design.

8. **Least customization of available off-the-shelf products:** There should be least customization of off-the-shelf products selected in the solution. Solution requirements should be achievable through configurations of the product. This is to facilitate easy upgrade of the base product with minimal retrofitting effort. Any costs involved in retrofitting of the Product upgrades shall be borne by the Bidder.
9. **Service orientation at the core of Architecture:** Solution architecture should be designed in a way that it is service oriented to promote reuse and ease of integration features.
10. **User configurable Rule engine**: Pension processing rules differ in each state. The proposed business rule engine should be extremely user friendly such that an IA&AD user, with little training, should be able to configure the rule set for an office. As the pension rules change, the IAAD (administrative/ designated) user should be able to update the rule engine in most cases on their own without assistance or minimal assistance from the SI or OEM.
11. **Easy to use Business Process Manager:** Business processes and users differ across states. Hence the BPM product should be able to provide extensive configurability as well as multi-tenancy features for segregating the business process configurations of each state. Also, it should be easy enough that an IA&AD technical user should be able to perform non-complex changes to the existing business processes with little training.
12. **Maximize Automation through appropriate tools:** Solution should use standard available tools for automating all aspects of CPP application development (viz. Product Backlog management, Code quality analysis, Security analysis, VAPT, Security and Performance testing, DevOps, Release management, etc.), MIS Reporting, SLA monitoring, etc.
13. **Self - service MIS Reports:** The solution should enable IA&AD users to self-design various Reports, based on information that will become part of the application.
14. **Cost efficiency:** Solution should consider cost efficiency as core parameter at all levels. Pay-as-you-go shall be a preferred costing model which involves horizontally equated cost distribution over the life of the project, as more states integrate to the solution. The solution should have a cost-effective model for all components involved in the solution, given the high volume of Pensioners / Users to be managed within the System. The volumes and concurrency of usage in the system is specified in Vol-1 Annexure D of this RFP.
15. **Portability –** Bidder must ensure that all the tools, technologies, frameworks, application source code, infrastructure components' configurations, software etc. used for development and deployment of CPP Applications must provide easy portability to any other CSP or on-prem

Datacentre. Any software licenses procured separately must also allow portability to the new environment. In case at the time of porting the applications to another CSP/On-prem Datacentre, some of the components/services/licenses/code are found to be incompatible, the Bidder shall bear the expenses related to providing an alternative solution.

1.2 Architecture Guidelines

Envisaged CPP Architecture is prescribed to follow IndEA framework. As outlined in IndEA framework the benefits envisaged by following the framework are supposed to be:

1. Provide a **unified experience** to the pensioners and IA&AD and State stakeholders, by offering integrated services.
2. Enhance the **efficiency** of processing, managing and delivery of pension services, by creating a fully digital platform and enforcing service levels of a very high order.
3. Improve the **effectiveness** of implementation of pension related policies and schemes by making it easy to change rules and offer variability at states level.
4. Enhance the **productivity** of IA&AD employees through easy access to required information at one place and a platform to manage grievances.
5. Provide integrated and cross-cutting services through seamless **interoperability** across the states in terms of Data, Rules and Processes.

Aligned to IndEA framework, envisaged CPP Architecture guidelines are discussed in following parts:

1. Functional Architecture
2. Application Architecture
3. Information Architecture
4. Infrastructure Architecture
5. Security Architecture

Functional Architecture shall cover the layered approach of functional components of the solution. Application and Infrastructure Architecture shall cover all Technology stacks and the hosting options, requirements etc. Information Architecture shall cover guidelines for managing Data. Security Architecture shall provide the guidelines and requirements of managing large set of users to the system and how to protect information through various layers.

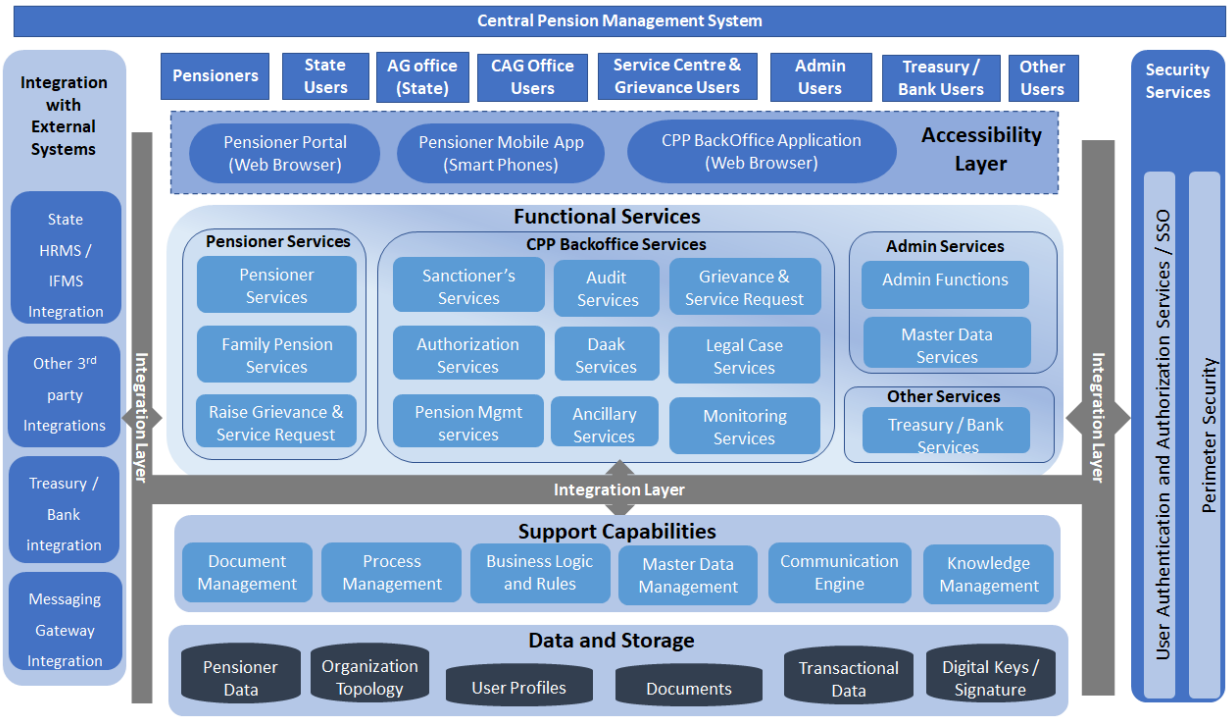
Based on the guidelines, bidders are encouraged to find the best fit solution meeting all criteria and adhere to the standards. Bidders will be scored on the merit of their Architecture, Design, Choice of platforms/ products, and all such technical criteria.

2 Functional Architecture

The Functional Architecture of CPP is envisaged as follows:

1. User Interface Layer
2. Accessibility Layer
3. Functional Services Layer
4. Integration Layer
5. Support Capabilities Layer
6. Data and Storage Layer
7. Security Layer

Below is the schematic depiction of the CPP Functional Architecture.



Guidelines for each of the seven layers are as following:

1. **User Interface Layer –** The User Interface Layer comprises of the various users that are intended to use the Pensioner Portal and CPP Backoffice application. RFP Vol-I Annexure A may be referred for understanding more details about these users and the applications.

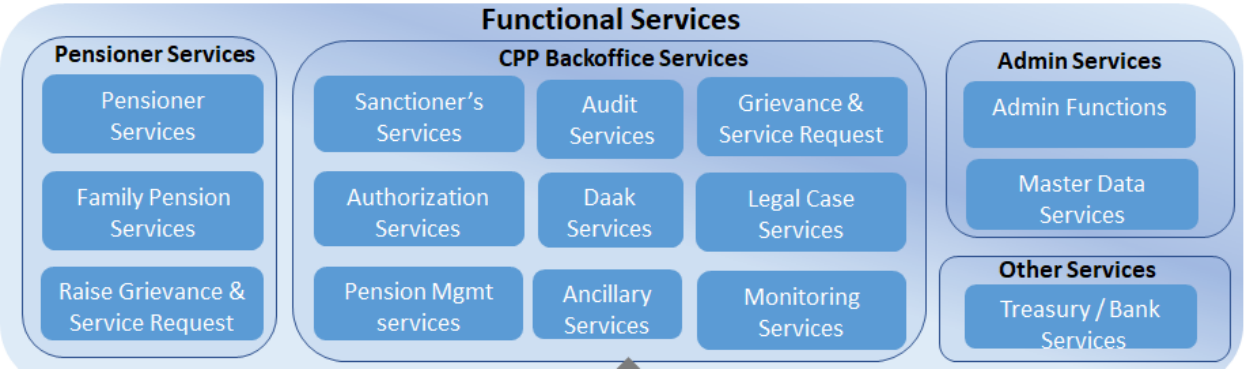
Users will have relevant access to the various application functionalities as per their assigned roles.

2. **Accessibility Layer** – This layer comprises of the various interfaces/ channels that would allow the users to access the various business functions of the CPP applications. CPP has been envisioned to have a web-based Back-office application for enabling the users to perform the various business functions pertaining to Pension processing and other related ancillary processes. The pensioners shall also be provided with a Web-based 'Pensioner Portal' as well as a Mobile app. The functionalities for each of these applications have been detailed in Vol 1 Annexure A of this RFP.

The solution should be designed such that access of CPP Backoffice application may be provided to its users through VPN, if required.

There should be a single domain name URL for CPP Backoffice Application and a single domain name URL for CPP Pensioner Portal. Any functionality / service accessed by any user/API/service, whether internally or externally, must adhere to these respective domain names only. In other words, there should not be re-direction of URL to any other domain/sub-domain while using any functionality/service of the aforesaid CPP Applications.

3. **Functional Services Layer -** This layer refers to the spectrum of services that will be used to serve the needs of digital pension processing throughout its lifecycle and to give secured, reliable, and transparent information to all stakeholders. These services should support seamless integration with all CPP applications and Mobile app.

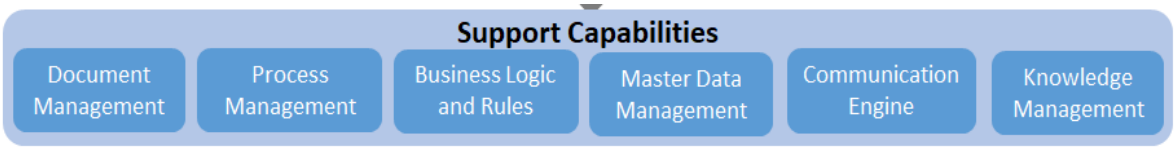


The various functional services have been compartmentalized into 4 zones for the various categories of users accessing the System:

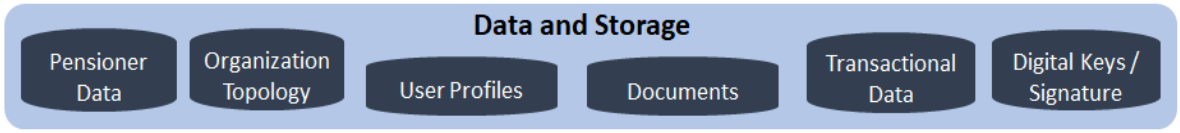
- **Pensioner services –** These will be available to the Pensioners through the Pensioner Portal and Pensioner Mobile App, and will provide all the business services pertaining to the Pensioner, such as Pension initiation for self and family pension (as may be applicable), viewing of approved PPOs, Raising Grievances and Service Request, etc.
- **CPP Backoffice Services –** These will be available to the Backoffice users such as State Users, AG Office users, CAG office, Service Centre, and Grievance redressal users, etc. for performing all Pension processing related business functions. It also comprises of other supporting functions such as Dak management, Recording of Legal cases, Audits, Dashboards, and reports for progress monitoring, etc.
- **Admin Services –** These functions will be used by the admin users for performing administrative activities such as Master Data management, Role/Group/User mapping, User provisioning and access control, etc.
- **Other Services** – These comprise of CPP Backoffice services made available to other external systems such as Treasury/Banks, etc. for accessing and updating information in CPP Backoffice application.

Detailed information on these aforesaid services is described in RFP Vol-1 Annexure A.

4. **Support Capabilities Layer –** Support capabilities layer denotes the landscape of required products and platforms in the solution landscape with key capabilities to support the functional services.



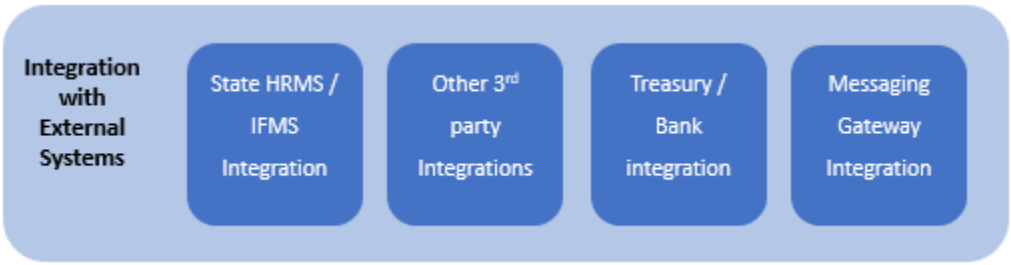
5. **Data and Storage Layer –** Data Storage layer of the system refers to the actual data of the application which will be used by the various CPP applications/services. Data shall comprise of entities such as Master data, Organizational topology related data, User profiles and the transactional data of the system. Data shall also comprise of Documents which need to be stored and managed in a uniform manner, Digital signatures, Activity logs, System configurations, etc. Aadhaar Data vault shall be required to securely store the Aadhaar numbers as per the guidelines published by UIDAI.



Since CPP shall manage data for multiple states, and data for each state must be accessed by that state only, hence multi-tenancy features should be used while managing data of each respective state. The CPP applications are more read intensive than write.

6. **Integration Layer** - The integration layer shall act as a bridge between the external and internal Applications as well as provide integration backbone for internal solution stack. The Solution must ensure assured delivery of messages and business transactions in a seamless manner.

   Below diagram schematically depicts key external integrations.



State HRMS/IFMS Integration– refers to a uniform mode and ease of integration with State Systems /Data (viz. State HRMS and IFMS systems, as applicable) as various states might have different states of maturity and data structure. This needs to be brought into a uniform and flexible

per state data structure. This integration may involve two-way communication with State Systems as well.

Other 3rd party Integrations– refers to the platform which would make it easy to host and support APIs that can securely communicate with other systems such as UIDAI Aadhaar, Digi-locker, IFMS/HRMS and other required systems in future.

Treasury / Bank Integration– refers to a uniform way of communicating with Treasury and Banks for disbursal of pension and its notifications. Entitlement of pension need to flow to such systems from CPP and notifications on status of disbursal need to be received by CPP for its record.

Messaging Gateway Integration– various status and information notifications would be sent by CPP to the end uses such as Pensioners and Backoffice users as SMS and/or Email. The messaging Gateway should offer a uniform mode of such notifications from the system.

7. **Security Services Layer** – Security Services layer denotes the services required for secured access of services, data, and user interfaces. Larger universe of users which are Pensioners can be viewed as consumers and need to be provided with the feature of two factor authentication while accessing interfaces. Other back-office users need to be provisioned with role-based access and authorization. System integrators are encouraged to look at the platforms / solutions which are cost effective in providing security features for the volume of users as specified in Annexure D. A directory-based user profile management should be preferred approach.

3 Application Architecture

This chapter outlines Application Reference Model (ARM), Technology capabilities to be built into the solution, expectations, and Application Architecture guidelines. Bidders are expected to follow the reference model and comply to the guidelines while suggesting a solution. Bidders are however free to choose exact platform / tool / product be it open source or commercial but must give a mapping with respect to the ARM and any departure from the ARM must be justified for.

3.1 Application Architecture Guidelines

Following Application Architecture considerations and guidelines must be followed by the bidders:

1. CPP is proposed to be a centrally deployed application, having Web Portal and Mobile interfaces, and integrated with other internal and external business services.
2. Ease of Configuration: Configurability is a must parameter specially for configuring and managing Business Rules and Processes, where-in relevant IA&AD stakeholders should be able to edit, change and manage rules in natural language like syntax. Stakeholders should be able to change the non-complex business processes on their own with adequate access rights. Also, with core business functionalities in place, the on-boarding of incremental States on the CPP system should ideally be accomplished through configurations only, with no/minimal code change.
3. Federated ecosystem of system users demands that solution supports multi-tenancy model in terms of managing Data, Rules, Processes and User Profiles.
4. Only authorized resources should be able to enable, disable or configure the different functionalities, based on Role Based Access Control (RBAC), but the application shall work on a common architecture, configuration, and functional modules.
5. Decoupling of business parameters/ workflows/ rules engine/ master data from the rest of solution architecture and making them configurable will allow flexibility.
6. Service Oriented Architecture should be the core of solution design. Most functionality to be offered to the users should be encapsulated and developed in the form of services.
7. The CPP Application should be designed such that it has a core framework over which various application functionalities shall be developed. This is to provide uniformity/standardization of application design within the entire application functions/modules as well as enhanced efficiency and manageability of application code.
8. The CPP should have an integrated core database, though there may be logical partitioning for effective data retrieval and storage. Further, the Database must be decoupled from the Application, and must be accessible through Data access APIs only, i.e. No application will access data directly from the Data storage.
9. The CPP application and its functionalities should be granular and modular enough for the administrators to manage access of the business functionalities for the various a CPP

users/groups/roles at any IA&AD office, at any given time, as per their requirement, without the need for a developer / code level change / custom UI change.

10. Ease of Use: Applications are easy to use, with a friendly, intuitive, customised UI for users requiring no specialised IT skills.
11. Sharing & Reusability: All commonly used Applications are abstracted to be built once and deployed across the Organisation through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.
12. Technology Independence: Application Design is open standards-based and technology-independent.
13. Application Security: Applications should be secure by design and developed using secure coding standards and practices.
14. Open-source software: CPP application shall prefer open standard software (OSS) to closed source software (CSS). CPP applications must comply by the "Policy on Adoption of Open-Source Software for Government of India". However, Enterprise level support shall be mandatory for all software provided in the system. For Further details, please refer to: http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf
15. Open Application Programming Interfaces (APIs): The CPP Application Architecture shall use Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations.
16. All applications must comply the "Policy on Open Application Programming Interfaces (APIs) for Government of India". For Further details, please refer to: http://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf
17. Specific OEM products may be used when necessary to achieve scale, performance, and reliability. Every such OEM component/service/product/framework/Managed Service must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system.
18. IA&AD envisions a custom-built solution to be developed for CPP Applications as part of this RFP. However, in case the Bidder proposes to use any existing product/platform/framework/accelerator and customize it for CPP, it must ensure that there are atleast 2 independent vendors/SIs/agencies (apart from the Bidder) who have implemented that product/platform successfully in atleast one similar-sized project each.

Bidder will be required to submit appropriate documentation, up to the satisfaction of IA&AD, testifying this condition.

19. Openness: Adoption of open API, open standards and wherever prudent open-source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable, and secure. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.
20. Platform & Database Agnostic: CPP Application shall be forward compatible. They shall be deployable on any technology platform and shall be able to communicate with any data store.
21. Secure Coding Practices: The CPP applications must adhere to Standard Secure Coding Practices. For example, while designing and implementing access management, session management, password protection, data protection, Error handling and log management, etc.
22. A QR code generator solution must be incorporated in the system to apply QR codes automatically on selected documents such as PPOs, etc.

3.1.1 Non-Functional Requirements for architecture

1. **Reliability**

   The system must have appropriate measures to ensure processing reliability for the data received or accessed through the solution. It will be necessary that the following issues be taken care properly.

   a. Prevent processing of duplicate incoming files/data
   b. Zero loss of data (data already saved *I* data at rest should also not be lost)
   c. Unauthorized access and alteration to the Data uploaded in the CPP system shall be prevented.

2. **Ease of Use**

   Ease of use such that applications are easy to use, with a friendly, intuitive, customised UI for users requiring no specialized IT skills.

3. **Multiple language Support**

   CPP must be able to capture data in various fields in multiple Unicode compliant languages. However, the UI of the web application (labels, messages, etc.) should be displayable in multiple Unicode compliant languages of Indian states that shall be on-boarded on CPP System as mentioned in the RFP Vol I scope. It should facilitate typing in vernacular languages, including the

facility for transliteration and also provide for a dictionary (with words being manually added by a user or uploaded from a csv/Excel file) to facilitate multi-language search. For Hindi, Devanagari script shall be used.

4. **Scalability**

   The CPP application should be able to scale elastically to handle the increase or decrease in workload. The Application must support load balancing and routing.

   The Application architecture must support horizontal scaling of Servers, compute, storage, network, etc.

   Graceful failure: The application must not have any Single point of failure. There must be a graceful degradation of services in case of any failure.

5. **Performance**

   The Application must comply by Service Response Time as required by the Application and stipulated in the SLAs. The Bidder must conduct Performance testing (preferably using automated tools) before every major release to ensure that the CPP Applications meet the expected performance benchmarks as specified in the SLAs.

6. **Security**

   Security solution for CPP architecture should comply with the specifications as stated in this document and the annexure C of Vol 1 of this RFP.

7. **Usability**

   The CPP applications must comply with ISO 9241-210:2010 Standards (Ergonomics of human-system interaction), GIGW Standards and other standards as stipulated by GoI.

8. **Quality**

   The applications should comply with industry standard Quality processes such as ISO/IEC 25010:2011 Systems and software engineering or CMM/CMMI guidelines for System and software quality models.

9. **Availability**

   All Applications must support the Availability SLAs as mentioned for each application.

10. **Recovery**

    The applications must comply by the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) as stipulated in the SLA.

11. **Error Handling & Resolution**

    The applications must efficient error handling. It must also provide detailed logs to enable efficient de-bugging and issue resolution. A repository of 'Known Issues' must be made available to the System Administrator.

12. **Documentation**

    All Software documentation including but not limited to following must be maintained with proper Version Control and Access Rights. Software Traceability Matrix must be maintained:

    a) SRS, Gap Analysis, Application Technical Design, Infrastructure Design, Testing, Use Cases, User Guides, etc.

    b) Project backlog, sprint backlog, release backlog, Executable specifications, retrospective document/ templates

    For more details, please refer RFP Vol 1.

    All documents exclusively produced for the project are the property of the IA&AD and cannot be reproduced or retained by the Bidder/ CSP. All appropriate project documentation will be given to IA&AD during and at the end of this contract or at the time of termination of the contract. The Bidder/CSP shall not release any project information without the written consent of IA&AD. Any request for information relating to the Project presented to the CSP must be submitted to the IA&AD for approval.

13. **Support for Differently Abled Users**

    All CPP applications must support accessibility by differently-abled Users and adhere to GIGW Standards.

14. **Change Control**

    The Product owner must approve and monitor the changes that are done to the software. All Change Request documents must be approved before implementation and Unit Testing.

3.2 Application Architecture Standards

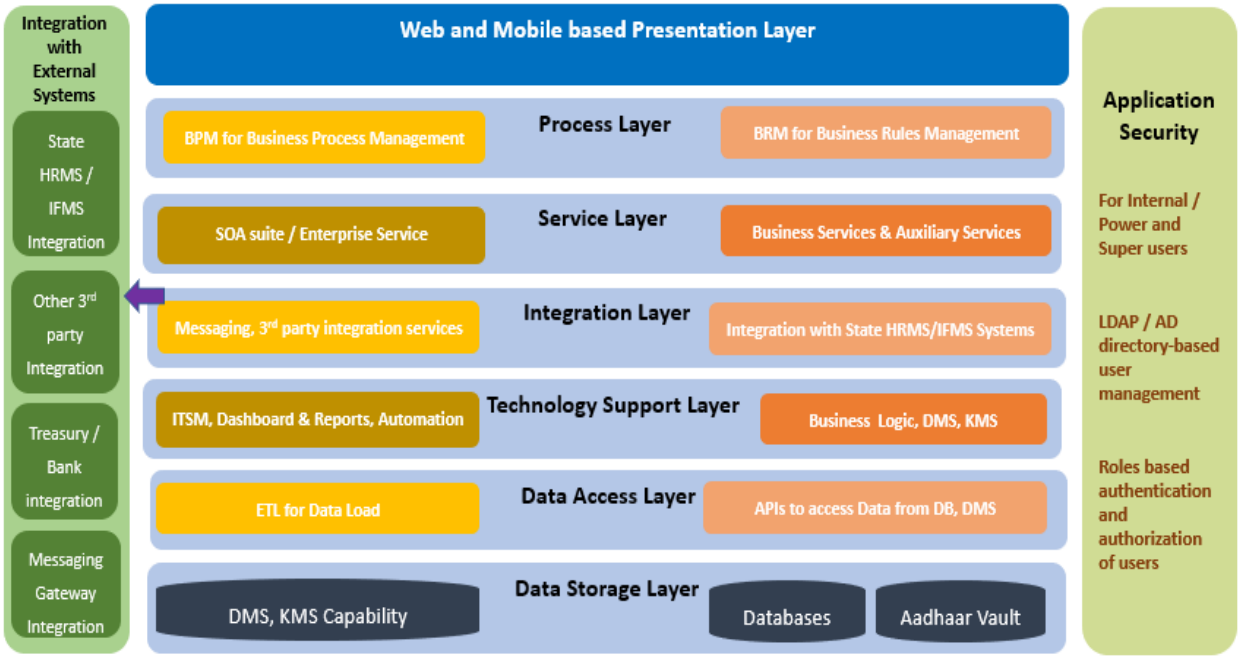
The envisaged IA&AD's Enterprise Application Architecture intends to ensure interoperability of all the applications in the system along with seamless upgradation/ migration and addition of new applications to the system. The Enterprise Application Architecture should adhere to applicable standards, such as:

a) **Interoperability Framework for e-Governance (IFEG):** http://egovstandards.gov.in/sites/default/files/Interoperability%20Framework%20For%20e-Governance%20(IFEG)%20Ver.1.0.pdf

b) **Technical Standards for Interoperability Framework for E-Governance in India:** http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf

3.3 Application Reference Model

Below is schematic depiction of 8-layer Application Architecture. Each layer is subsequently discussed in terms of their objectives and CPP requirements.



Layers of Application Architecture are as following:

1. Presentation Layer
2. Process Layer
3. Service Layer
4. Integration Layer
5. Technology Support Layer
6. Data Access Layer
7. Data Storage Layer

8. Security Layer

3.3.1 Presentation Layer

Presentation Layer consists of an easy-to-use web-based interface for various stakeholders as well as mobile based interface for the pensioners.

Bidders must follow the following guidelines while choosing for a Technology at Presentation layer and designing for a solution.

1. Presentation Layer must be light weight and easy to use interface mostly following one page paradigm for one action.
2. It should follow as less the number of clicks for users as much possible.
3. Presentation Layer should cater to multilingual needs and users should be able to choose the language of their choice.
4. UI should be form-agnostic and should be self-aligning to several form factors.
5. Simple to use is the key and must exhibit high level of performance while being accessed.
6. Presentation Layer must provide uniform interface and should not take users to multiple presentations of different tools.
7. There should be role-based access to the user interfaces and only designated roles should be able to access the user interfaces they are required for.
8. User interface must be able to present customizable, user/role specific dashboards and drill-down reports.
9. The application must provide Portal specific functionalities such as Login page, Landing page and other custom-made web pages/forms for enabling the access of various functionalities to its various users/roles.
10. User interfaces should be browser agonistic; should support atleast Mozilla, Chrome, Safari and Internet Explorer.
11. Mobile based interfaces should be supported atleast on iOs and Android.
12. Presentation layer should be decoupled from the underlying service or process layers and must communicate in terms of API / service calls. Process Layer

Application Architecture is suggested to follow a decoupled approach in terms of Business Processes, Business Rules and the Business Services. These platforms are preferred to be integrated seamlessly and through API based approach or messaging. In case, bidder adopts for a platform which has more than one

of these layers built-in, bidder must design the solution carefully where decoupling of layers is maintained. Process Layer consists of Business Processes and Business Rules in a way that users with appropriate permissions are given flexibility to change processes and rules. Bidders should consider following guidelines while designing solution for Business Process and Rules layer.

1. Business Processes will be long running and will have multiple manual intervention steps.
2. Business Process Management layer should provide user friendly dashboards, automated notifications should be sent through email as well as SMS wherever applicable.
3. There could be variation in Processes for each state and this should be incorporable in the master process. Thus, multi tenancy feature must be available.
4. Processes must be secured with role-based authorization so that no unintended stakeholder attends to the manual steps by mistake.
5. A personalized inbox feature should be supported for the stakeholders.
6. Business Processes should be guided by the Business Rules Engine for decision making and calculations.
7. Business Process Layer and Services layer should be decoupled, allowing reusability and consumption of services from Process Layer.
8. It should be possible to attach SLA to each step of the processes, get alerts of violation and in-built escalation triggers.
9. It should be possible to monitor ongoing business Processes.
10. BPM platform should offer an activity monitoring dashboard with pre-defined reports around processes, actors, violations, SLA adherence etc.

Bidders should similarly follow a guideline while suggesting a Business Rules Management platform in the solution.

1. Business Rule Management (BRM) platform must support UI based interface for authoring, editing, or deleting of rules.
2. Multiple versions of the rules and their effective change date should be supported by the platform.
3. Suggested BRM platform should be seamlessly integrable with the BPM tool and API based accessible by the Business Services at Services layer.
4. BRM platform should support role-based access control.
5. BRM platform must support multi-tenancy.

3.3.2 Service Layer

CPP Application Architecture should enable a set of well-defined services to various stakeholders based on functionality (as described in Vol 1 of this RFP). Following can be considered as the broad group of services:

- Pensioner services
- Sanctioning Services
- Authorization services
- Audit Services
- Bank and Treasury Services
- Master Data Services
- Monitoring and Ancillary Services
- Grievance Management Services

Cross-cutting functionalities of the application shall be designed to deliver the set of related services in an orchestrated manner for multiple state requirements of managing Pension lifecycle. All the applications shall inter-operate to the extent needed, mostly through the Open APIs. RFP Vol 1 Annexure A provides details of CPP functionalities.

Some of the auxiliary services should be considered as –

- **SMS services:** SMSs are envisaged to be sent to pensioners, intimating various stages of processing like receipt of application in CPP, authorisation/return of case etc. The SMS services shall need to be in high redundancy mode, preferably with 2 different Service providers.
- **Email service:** NIC Email services are envisaged to be used as a part of the solution to send alert/ intimations / automated messages to the registered email ids, based on preferences set up/ opted by individual users.
- **QR Code:** QR codes are envisaged to be part of solution for all the outputs generated from the CPP system.

3.3.3 Integration Layer

Integration backbone in Technology Landscape brings interoperability and easy access to information and business functions across different IT components/applications. This layer provides the capabilities

required for enabling Service Oriented Architecture (SOA) that involves service designing and publishing, routing, protocol support and conversion, data transformation, messaging, etc. in a heterogeneous environment where services are accessed between two IT components to achieve the required business function.

In CPP, Integration should be seen from two perspectives – internal integration backbone and external integration interfaces, e.g. state pension application systems, IFMS, Treasury, Bank, Aadhaar, PAN etc. State Integration Guidelines. These integrations may have push-pull capabilities and may involve real-time exchange of data.

CPP is a central Pension Management System. While there is large part of solution is common, different states will be onboarded with difference in data attributes, logic, rules, processes, and organizational topology in the sense of approvers and sanctioners. Thus, a state integration must be seen in the light of:

a) Master Data of retiree from the state and other related data
b) User profile and access control rights set up
c) Business rules specific for the state
d) Business Processes specific for the state (Business Processes may vary marginally from State to State)

State Integration should be more of plug-and-play modular extension work than change in any code. It should necessarily not invite any customization or change in code, rather provide all features by configuration. It is important for the bidder to craft the solution by making all four integration points configurable in the solution.

3.3.4 Technology Support Layer

Technology Support Layer refers to the core support capabilities in application landscape Following technological capabilities are to be considered as part of solution.

1. Business services
2. Document management Capability
3. Knowledge management Capability
4. Tools based Dashboard and MIS Reporting capability
5. ITSM compliant tool
6. Automation capabilities

Bidders should prefer to achieve above capabilities through standard platforms or products than custom development. A guideline for each of the capabilities is given as below.

1. **Business services:**

   This comprises of the back-end business logic which resides in the form of Application code and is invoked during the execution of Business Processes established using BPM as well as Business Rules configured in BRM. These services interact with other Technology support services like Database, DMS solution, etc. and the Integration layer services etc. to serve the requests coming in from the end-users via the Web layer.

2. **Document Management Capability**:

   Solution should provide for a mechanism to upload / store the documents pertaining to the Pension cases and be available for other users within the CPP application. A basic document management capability is thus required in the solution. Document Management capability should further allow for role-based access of documents and should not be directly accessible by any user interfaces for protection. Once the Pension approval process is complete and PPO is issued, the Documents pertaining to that pension application become “permanent records”. Majority of pension documents fall in this category of “permanent records”. These records may be stored in a lesser performance oriented but large capacity-oriented storage for efficient usage of the infrastructure.

3. **Knowledge Management System Capability**

   A basic feature of knowledge management should be facilitated on the solution by which back-office users are able to look for rules, changes in rules, rulings, circulars and certain calculations if they want to as easy reference. Such Knowledge Management feature should be integrated with the user interface provided for the back-office users.

4. **Tools based Dashboard and MIS Reporting capability**

   Dashboards and MIS Reporting is a mandatory feature of any solution in terms of business, audit and monitoring related reports. While a set of standard reports will largely be used part of the

solution, bidders are encouraged to opt for a tool-based reporting capability that offers visualization and self-service reporting to its users.

5. ITSM compliant tool:

A standard ITSM tool must be provided for easy management of IT technical support related incidents that would:

a) Provide a standard and easy interface for logging of the incidents.

b) Each of the incident must be allowed to follow a configurable lifecycle and escalation matrix.

c) The platform should enable auto notification via email and SMS for resolution and closure of the incidents.

d) Resolver of the incidents and service requests should be able to prioritize and forward to another desk for resolution.

e) Tool should allow for retention and archival of the incidents and service requests for audit purposes.

f) ITSM tool shall provide access (user-ids) to few users in each state to log defects/incidents and to know the resolution statuses of these incidents.

g) ITSM tool should provide an auto-ticket generation feature for occurrence of any event that has characteristics deviating from the SLA parameters in the system. Such events should be configurable in the ITSM tool for auto-ticket generation / closure.

h) CPP System related Change requests to be logged & tracked in ITSM.

i) The platform chosen should provide API based integration with various systems such as Enterprise Monitoring tool, Messaging Gateway, Service Layer, Automation Layer and User management layer etc.

j) Bidder shall deploy different instances of ITSM tool in Production and Pre-production (Staging) environments to allow logging and reporting of incidents for each of the environments separately.

6. Automation Capabilities

While solution is largely process driven in terms of business processes, there could be many administrative tasks such as user provisioning, assigning of tickets opened in ITSM tool, auto

resolution of standard set of queries/ incidents etc. that can be supported using automation capabilities. IA&AD would like to leverage such technologies for smooth and efficient operations of CPP solution. However, any extensive use of Artificial Intelligence or Business Analytics is not in scope of the project.

3.3.5 Data Access Layer

Data should be accessible to the business and integration services only through a Data Access Layer that provides abstraction, independence, and interoperability from the underlying Data Management and Data Storage platforms. The design must provide coherent and standard mechanisms for managing and accessing the data, preferably using APIs/Services. The data from the databases or file servers should not be accessible for read or write operations by any other means except through the APIs/services of the Data access layer.

3.3.6 Data Storage Layer

Data Storage Layer in the context of Application Architecture refers to the Data Storage and Management platforms, such as Databases, File repositories, etc. Nature and needs of Information, however, is explained in section 4 on Information Architecture guidelines.

Data Management platform should be seen independent of the rest of the solutions and bidders should freely adopt the best of the technology keeping below guidelines in mind:

1. Solution is more read intensive than write and most data of Pensioner once the application is processed will remain inactive and only for view.
2. Most data about pensioners may be accessed anytime and over any number of years and thus bidders should not assume data to be archived after few years.
3. Bidders can openly evaluate between SQL and NO-SQL databases basis merit of performance, manageability, and scalability.
4. Different states will share several attributes in common but may also considerably vary in terms of additional attributes. Thus, a multi tenancy feature is inherent in the solution.
5. Number of pensioners though appear to be as high as multi million, but associated data for each Pensioner is not assumed to be large. Annexure D of RFP Vol 1 should be referred for sizing details.
6. Data must be stored in most secured way and should be accessible through strict role-based access control mechanism.

7. Platform that requires high level of housekeeping activities and are prone to database level locks should be avoided.
8. Data Management platform must run in High Availability mode and should allow for continuous replication to the Secondary Datacentre (DC-2).
9. Data storage should have multi-tier facility where active data could be stored in a fast / hot storage, while less frequently used read-only data could be moved to lower performance storages for achieving cost and performance efficiency. Active data here refers to the data pertaining to pension applications in progress as well as applications whose PPOs have been issued in the last 1 year from current date. However, the end-users should still be able to access the information older than 1 year whenever required in real-time, from the CPP Applications.

3.3.7 Security Layer

Security Layer in terms of Application Architecture refers to the platforms and technology capabilities to support security at various levels inclusive user profile and access and authorization management, role-based access and authorization at each layer of the application. Bidders should follow the following guidelines while designing for this layer in the application landscape.

1. A platform-based approach is preferred than a custom solution for managing users be it external or internal users.
2. Directory services is a preferred approach for its advantages and advances in terms of user management.
3. There should be self-service feature for the system administrators and super users to provision and deprovision user profiles in particular roles with necessary access controls.

For further details on Security requirements, please refer Section 6 of this document.

4 Information Architecture

Data architecture provides a mechanism for the IA&AD and State users at various levels to identify, discover, describe, manage, protect, and share the data, reuse information consistently within the CPP applications.

4.1 Principles

Bidders are expected to consider the outlined Data Management principles and relate it to the context of CPP.

1. **Data Asset**: Data is an asset that has a specific and measurable value to the department and is managed accordingly. The universe of Retiree once created would be an asset to the IA&AD as well as other Government departments. Information created is long lived and is critical to provide traceability of the processing, entitlement, and revision of pension of the Pensioners registered in the system. It is expected that claims may be filed by the beneficiaries of the Pensioners even after very long period and hence there is no purging of information envisaged in the system.
2. **Data-sharing**: Data is shared across IA&AD, subject to rights and privileges, to prevent creation and maintenance of duplicative sets of data. In the context of CPP, Data is provided by the states and once data is transferred from the State HRMS/IFMS Applications, it is proposed to serve as the single source of truth for all stakeholders once it is imported into the CPP application.
3. **Data Security**: Data is protected from unauthorised or unlawful processing, accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive data. Rules regarding storage of AADHAR and other personal information of pensioners should be strictly adhered to. Implication of this principle on CPP is that Data must be enabled with role-based access control mechanism. Sensitive information like Aadhar is not supposed to be stored directly and Aadhar Data Vault is supposed to be used instead for the purpose.
4. **Security Policy Document**: The Bidder shall be required to submit a Security policy document detailing the various user security related attributes and guidelines, and mechanisms of secured access of Production systems to the O&M team.

4.2 Document Storage capabilities

The proposed CPP solution should support storage of digital documents in any format support roles and rights-based security where there can be multiple levels of access right to the content like read, create, modify, delete, etc. The proposed solution should ensure secured access to the documents only by the authorized parties. Authorized Users should be able to add documents to the Document repository along with relevant meta-data pertaining to each of those documents and retrieve the required document by performing “Search” operation using these meta-data parameters.

4.3 Data Standardization and Master Data Management

Master Data is critical to in the context of CPP to ensure that all states use a standard set of data and thus the centralized application is able to interoperate in a meaningful manner. The Master Data management is to be delegated to IA&AD privileged users. It should be ensured that users do not maintain their own list of values or manage a copy of their own. Data duplication must be avoided hence a data dedupe mechanism should be built in the solution.

5 Infrastructure Architecture

This section details the guidelines for IT Infrastructure for the Centralized Pension Processing (CPP) system. It includes the guiding principles of required Infrastructure to support the Application Reference Model (ARM), hosting options and Disaster Recovery requirements. System Integrators are expected to respond with a solution of their choice that adheres to the Preferences, Guidelines, Considerations, and Requirements.

5.1 Infrastructure Guiding Principles, Considerations and Preferences

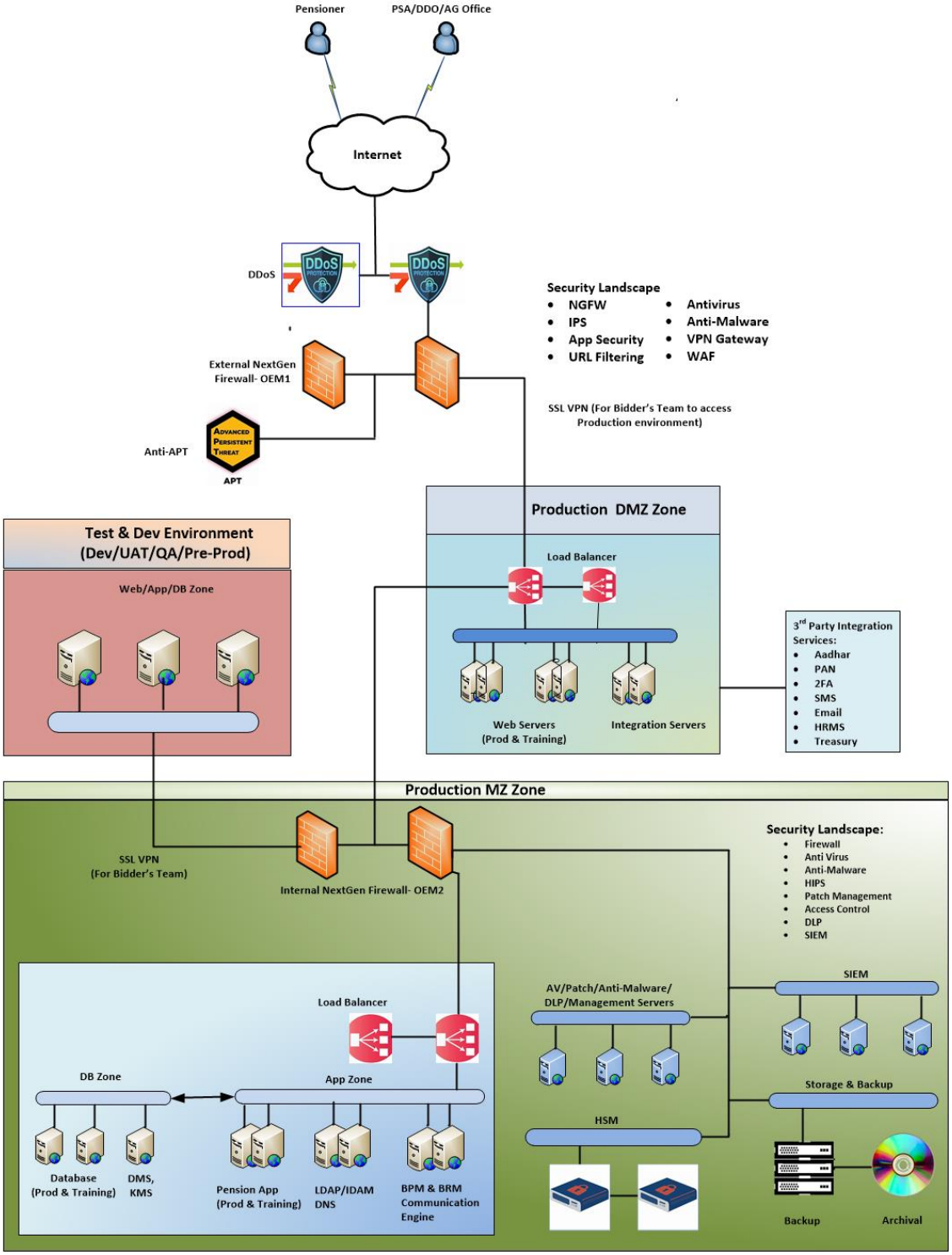
Bidders are expected to consider the listed guiding principle and adhere to them in their solution.

1. T**echnology Independent Architecture**: need to be developed in a technology-neutral manner to avoid captivity to a specific product or implementation method.
2. **Future-proof Architecture**: CPP need to be suitably designed and developed to be future- proof, not requiring frequent revisions with the advent of every new technology.
3. **Open Standards**: Open Standards need to be adopted in the design and implementation of CPP.
4. **Provider independence:** Bidder should ensure that there is portability of the solution. Portability shall include migrating the solution/application (along with data) to a different SI or CSP.
5. **Scalable environment with pay-as-you-go model:** As the system scale with time with more states being onboarded, it is expected that the environment provided by the provider is scalable and in pay-as-you-go model.
6. **Platform-as-a-service a preferred model:** Most Technology capabilities are expected to be offered in Platform-as-a-service model. For this, bidder may refer to the Technology Support Layer of the Application Reference Model (section 3.2.5 of this document). Even if some of the Technology Platforms are not provided in PaaS model by the CSP, the System Integrators are encouraged to bundle it as PaaS to IA&AD.

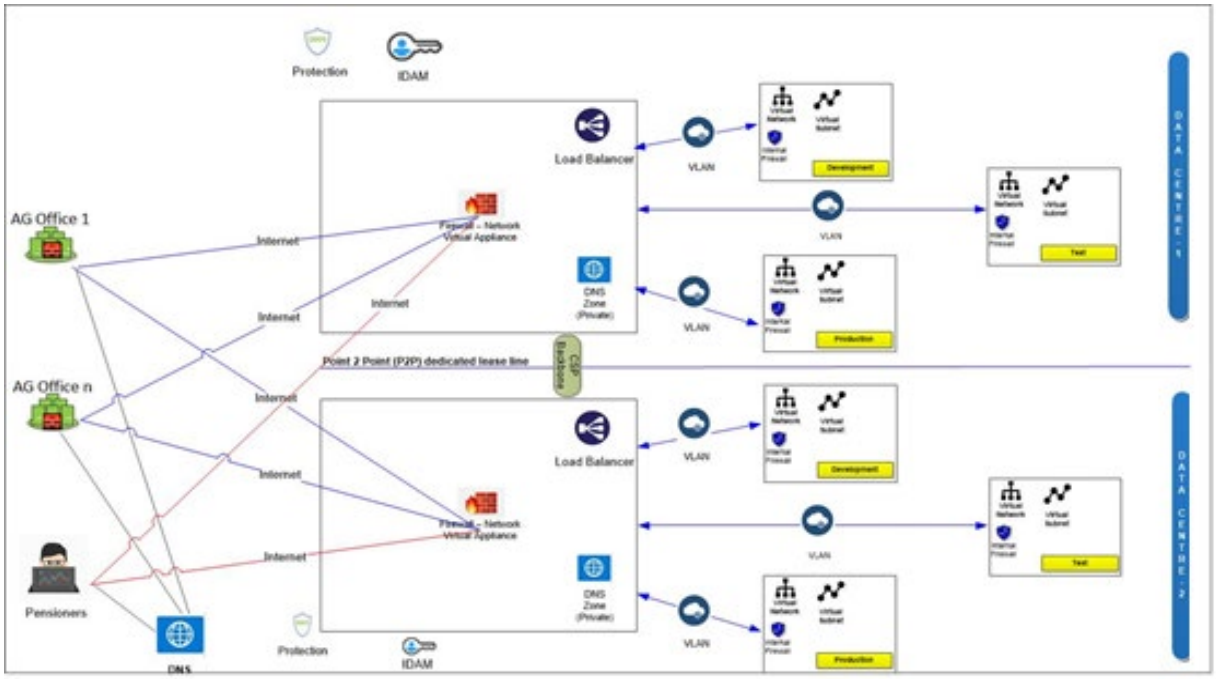
7. **SLA driven manageability:** Since it will be a CSP model for Infrastructure hosting, all the manageability parameters will be strictly measured on SLAs. For SLA the bidder may refer to the Annexure Ao f the RFP Vol 3.
8. **No single point of failure:** All components / services (hardware and software), which are required to be provisioned in HA mode in Production environment, should be configured so that there is no single point of failure in the system. It should further be load balanced at each level.
9. **Business Continuity with no data loss:** Data replication between Primary and Secondary Datacentres must be a continuous process as per the stated RPO.
10. **Security and privacy:** Access to the hosting environment must be secured so that there is no access of the control console to any unauthorized party.
11. **Credentials of the Proposed IT infrastructure:** The IT infrastructure components/product/services proposed for CPP project should be present atleast once in the latest two published Magic Quadrant of Gartner's / Forrester Wave reports. This is applicable only for those components where it is explicitly listed as a compliance requirement in Vol 1 Annexure C of this RFP.
    - Bidder should consider the latest two Gartner/Forrester report published on or before last date of bid submission. Any reports published after that should not be considered.
    - Bidder needs to submit a copy of relevant section of the Gartner/Forrester report along with technical proposal.

5.2 Deployment Architecture

A reference deployment architecture for CPP application is depicted below.



There may be certain components that are provided as part of inherent Cloud security, and therefore may not be required to be provisioned separately. However, it must be ensured by the Bidder that all the aspects of the above reference deployment architecture are eventually met. An illustrative network diagram of a Cloud Service Provider (CSP) may be referred as below.



Bidders need to provide Cloud Hosted Deployment Architecture. Minimum requirement of Cloud hosted option that bidders choose are as below:

1. Cloud Service Provider (CSP) must be MeiTY empanelled.
2. The CSP should have Datacentres at different physical locations in order to provide cloud Service offerings & Cloud Disaster recovery services.
3. Primary DC (DC-1) and Secondary DC (DC-2) should be provided in VPC (Virtual Private Cloud) model and no data should reside outside India.
4. There must be continuous data replication between DC-1 and DC-2 as per stated RPO.
5. Appropriate and periodic Back-ups must be enabled at both DCs.
6. Bidders should clearly list the common services in VPC model provided by the CSP along with SLA. SLAs should be adhered to minimum as outlined in Vol 3 Annexure A of this RFP.
7. An illustrative deployment Architecture of a Datacentre hosted on Cloud is prescribed diagrammatically, however, bidders are expected to propose for the CPP IT infrastructure deployment architecture to meet the required security guidelines and SLA as per the RFP.

8. Cloud hosted production environment should be hosted in different Virtual Network zone separated from all other environments within the Private Cloud to ensure that the production environment is segregated. Similar approach should be followed for both DC sites.
9. Deployment Architecture is preferred to follow a hub-and-spoke architecture, wherein all traffic filtered at perimeter security layer converges to the Hub Firewall and subsequently distributed to the different VLANs.
10. There should be no single point of failure in terms of any equipment, server or storage in the entire Infrastructure stack and this must be ensured by providing High Availability mode at each level in Production environment.
11. CSP must be certified as minimum Tier-3 Datacentre.
12. Monitoring dashboards must be made available by CSP and to the required extent by IA&AD.

Bidders should take a note that there is no concept of 50% or less Secondary Datacentre (DC-2) in this solution. DC-2 should be considered 100% but activated and paid for only when disaster is declared or during the DR drills. Continuous data replication must however be factored in. DC-1 and DC-2 should follow like to like Architecture and capacity and in terms of all the environments required to be provisioned for the CPP project.

The guiding principles followed in CSP centric deployment architecture are:

1. Elasticity in the system: It should be able to scale as need be, as it is expected that the states will be onboarded in a phased manner.
2. Ease of Management: CSPs are expected to provide smooth manageability experience and with tight SLA monitoring. Most common services of Network, Security and Infrastructure are expected to be offered off-the-shelf by the CSPs.
3. Quality of Service: CSPs should provide certified credentials about the quality of services provided by them and should demonstrate these capabilities/certificates during their technical presentation.
4. Best-in-class technology and Technology independence: CSPs are expected to provide the best-in-class technologies in terms of equipment, servers etc. and will be refreshing them as and when needed, effectively providing a platform independent solution to IA&AD.
5. The Cloud centric deployment and preference for Platform-as-a-service (PaaS) model will be accorded.

5.3 Environments to be provisioned

Bidder must provision for the following environments as a part of its Infrastructure design, setup, and BoQ at Primary Datacentre (DC-1):

1) Development
2) Testing (QA)
3) User Acceptance Testing (UAT)
4) Training
5) Pre-Production
6) Production

The Secondary Datacentre (DC-2) must provision for a minimum of Development, UAT, Training and Production environments.

5.4 Infrastructure Services Requirements

This section further details Infrastructure requirements that bidders should meet.

1. Bidder needs to size the solution components to meet the project requirement. Bidders must arrive at their BoM based on their analysis of the Functional requirements and other requirements as mentioned in this RFP. Bidders may provide any additional items, beyond what is mentioned in the indicative BoM of this RFP, in their bid with proper justifications in their technical design.
2. In case of any component / services not meeting the SLA, the Bidder must upgrade the services within the stipulated time as per SLA. Such upgradation of services, which are in the event of not meeting performance criteria, IA&AD is not liable for any additional payment. In case of failing to do so, bidder will be liable for a penalty as outlined in the RFP.
3. All Infrastructure services must be available in High Availability mode, to make it fail safe. Also, bidder must meet availability SLA as outlined in the RFP. Bidder must size and choose Cloud services carefully, in order to meet SLA requirements.
4. Internet connections need to be sized for adequate bandwidth and with redundancy. Network should have fail-over path for each line for both the DCs.
5. The proposed systems should be of enterprise class and must be of current/stable version as per OEMs offerings, in line with advancements of technology in these domains at the time of implementation. Bidder needs to provide the published benchmarks for the stated systems

along with the sizing assessment sheet being certified by the OEM/ Bidder (as applicable) for the stated systems. All the components should be able to handle expected loads and provision the desired transaction times and throughputs.

6. It is to be noted that bidder needs to provide a detailed assessment sheet taking into considerations the volumetric and other details given in the RFP, including the capabilities to provide the desired scalability in-line with projected growth in volumes and traffic. The assessment should clearly highlight the sizing parameters taken into consideration while designing the solution and also should be provided on OEM / Bidder letter head, along with publicly available published benchmarks.
7. Bidders should preferably look for Database as Service option with scalability, and continuous replication. It must be a secured database. Bidder must provide logic and examples of similar applications for choosing a Database option, along with benchmark figures. Database must be reliable and ensure no data loss. It must enable role-based access.
8. The systems architecture should clearly demonstrate and highlight the key requirements of IA&AD viz reliability, availability, scalability, survivability, resilience and serviceability of individual critical components as well as the CPP system as a whole.
9. Bidder needs to comply with the availability requirements as stated in the SLA (Annexure to Volume- 3 for RFP) for the CPP system.
10. Bidder must provide Application Technical support during Prime Business Hours. There should be a systematic process of monitoring, logging, resolving and closing the issues in production environment. The process and tool must be demonstrated and described during the bid process.
11. All necessary tools for monitoring and measuring the service levels with respect to application performance, server performance, resource utilization, storage performance and utilization and network throughput must be provisioned as part of the infrastructure. The tools should be capable of collecting and providing all the necessary information from all the infrastructure components for generating detailed MIS reports for various periods and parameters of reporting.
12. Solution should provide access to IA&AD System administrators to review and monitor the performance, utilization and security compliance of the provisioned resources. The Bidder should provision for atleast 5 users from IA&AD for performing these functions.
13. Networking service should be capable of processing IPv4 & IPv6 traffic. Security features that are delivered shall be IPv6 ready. All devices should be IPv4 and IPv6 ready from day 1. The

proposed solution and all appliances should meet this requirement. The Bidder shall also be responsible for security adherence on both IPv4 and IPv6.

14. Bidder should prefer PaaS (Platform-as-a-service) over IaaS (Infrastructure-as-a-service) to make it a managed service in true sense.
15. Patch management: Bidder must ensure that all hardware and software components in use are subjected to periodic and regular patch management as per SLA.
16. The Primary Datacentre (DC-1) and Secondary Datacentre (DC-2) should be architected in such a way that any of the modules may be run from any these datacentres, without any impact on the SLAs being defined.
17. All the material/platforms/software provided as a service for CPP application should be enterprise class, to handle expected loads and provision the desired transaction times and throughputs.
18. OEM product upgrades due to technology adoption or other reasons should support backward and forward compatibility without any additional effort/cost to IA&AD.
19. Bidders may use open source, but it should be fully supported and managed service.
20. All the environments listed in this RFP must be available within the timelines specified in the RFP Volume 1.
21. Bidder shall be responsible for Procurement and management of DNS and SSL certificates for the CPP project.

5.5 CPP Network Infrastructure Requirements

CPP Application will be used by the users as mentioned below:

1. Back-office staff (AG offices, DDOs, PSAs, etc.) will connect to Datacentre through Internet.
2. Pensioners will connect to Web-Based Pensioner portal application and mobile app through Internet.
3. Trainees/Trainers will access Training environments through Internet.
4. The Development, Testing and O&M team will access the various Production and Non-Production environments via VPN.

NOTE: IA&AD may decide to exercise the option of engaging VPN Services for AG office users as an added security requirement. The timeline for VPN implementation shall be decided by IA&AD as and when required.

Bidder shall ensure dedicated high-speed connectivity between DC-1 and DC-2 (with appropriate redundancy), as well as appropriate bandwidth for providing seamless access for all the users using the CPP Applications (Pensioner Portal as well as CPP Backoffice application).

The web based CPP application will be exposed to Internet for business users. An indicative **minimum** bandwidth requirement for Internet connection (to be provisioned at CSP Datacentres) as per IA&AD estimation is shown in following table:

Link Required At	Minimum Bandwidth requirement in Mbps	Number of links	Redundancy Requirements
DC-1	100	2	With different ISPs.
DC-2	100	2	With different ISPs.

The Bidder would ensure the following:

a. There is some direct leased-line connections between DC-1 & DC-2 keeping in view that near real-time replication of storage and Databases between the two datacentres is required as per the RTO and RPO. The Bidder is required to carry out independent assessment of bandwidth requirement based on the data replication requirement, user projections for entire contract duration. The performance of the CPP Applications would be driven by the performance parameters stated in the SLA. Any variation between actual and indicative bandwidth requirement would not confer Bidder any right to seek deviation(s) from the performance parameters stated in the SLA. Bidder may propose bandwidth in scalable model also. But the Bidder need to meet the service levels as mentioned in this RFP for the entire duration of the project.

b. The Bidder must ensure redundancy of network bandwidth link for each connection mentioned above. Also, Bidder must ensure that the aforesaid bandwidth link redundancies are provisioned from two different Service providers. This is to ensure two landings of network connectivity at each site. While links at each site are supposed to work in load sharing mode, the individual link for each location should be able to cater to the bandwidth requirement even if the secondary link is down. The redundant links at any location must not be overlapped on the same media by two service providers.

c. Bidder needs to provide details of bandwidth sizing for each link in its technical proposal. Including the detailed Bandwidth calculation and should ensure that bandwidth utilization should not cross 70% at any point of time. During the operations if bandwidth utilization reaches 70%, Bidder will be required to increase the Bandwidth. Bidder shall be liable for penalties arising out of Application performance below specified service levels (specially for end-users) due to inaccurate bandwidth proposed/provisioned.

d. In its technical proposal the bidder needs to provide the details of bandwidth service provider (bandwidth service provider name) from whom it is going to provide bandwidth services, or the business arrangement between the Internet Service Provider, CSP and the Bidder.

e. The Bidder through EMS should also provide network related reports including the below:

   i. Link up/down (real-time as well as periodic)

   ii. Link utilization in % (real-time as well as periodic) (Link utilization should not be more than 70% in each case, barring acceptable occasional surges)

   iii. Top and Bottom N graphs showing the best and worst links in terms of availability (periodic)

   iv. Reports on threshold violations. Provisions for setting thresholds and getting alerts on threshold violations should be there in the system. (real-time as well as periodic)

   v. Bandwidth utilization report for each link and utilization trends. The report should have provisions for displaying the minimum, maximum and average for each link. (real-time as well as periodic)

   vi. Application/port level traffic analysis with source and destination identifications

   vii. Report on jitters, latency' due to network parameters, closely linked to reachability shall be available. (real-time as well as periodic)

5.6 Performance Management and Monitoring

Performance Management involves monitoring, collecting the required resource utilization metrics and tuning of virtual resources. In addition, in a virtual environment, devices can be added, removed and load balanced for managing the required levels of performance. Also, configurations of the logical partitions and virtual environments may be tuned for performance optimization. Processes / Services may also be moved seamlessly to maintain the levels of performance.

The EMS module of the CPP Applications should be able to monitor the set of performance objectives for the Bidder. Typically, this set of objectives includes system and security resources such as CPU, Memory, process, storage, utilization, configuration changes or any other parameters. The Bidder is required to:

1. Perform the virtual environment/device availability monitoring
2. Perform the virtual device alert monitoring
3. Perform the configuration change and log monitoring
4. Monitor the virtual device access to ensure the continuous CIDR operation
5. Monitor the performance of the virtual server/ device and highly available systems
6. Monitor the utilization of resources (CPU, Memory, Storage) and network connectivity
7. Monitor the physical server capacity and distribution of virtual servers
8. Proactive identify security vulnerabilities and potential threats
9. Monitor the SLAs on a periodic basis and take timely corrective action wherever necessary.

5.7 Business Continuity Planning and Disaster Recovery

In order to ensure continuous availability of the applications along with complete managed services and disaster recovery services in case of disaster at Primary Datacentre (DC-1), IA&AD wishes to provision a Secondary Disaster recovery service (DC-2) as well on same CSP. The said DC-2 infrastructure is envisaged to enable IA&AD to deliver services effectively to its stakeholders even in case of disaster at DC-1. Bidder shall prepare the Business Continuity Plan for the CPP Application in compliance with ISO 22301:2012 - Business Continuity Management System and submit the necessary documentation to IA&AD. The purpose of business continuity/disaster recovery is to enable CPP to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities.

BCP plan should have minimum four main components:

i. Emergency procedures – describing the immediate action to be taken following a major incident that jeopardizes business operations.
ii. Fallback procedures – describing the action to be taken to move essential business activities or support services to temporary locations.
iii. Resumption procedures – describing the action to be taken to return the business to the normal full operation, usually at the original site.
iv. Test schedule – which states how the plan should be tested.

BCP should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster. Incident response plans should be developed by the Bidder which should include impacted users and other business relationships that represent critical business process dependencies. Each level of plan should have a specific custodian. The Bidder would be responsible for identifying and applying changes to the BCP as part of process optimization initiative. The complete plan should be reviewed at least annually. Copies of each of the above business continuity plans should be held off site.

The Bidder should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes pertaining to the CPP Application. Bidder shall conduct training(s) for the personnel involved in Disaster Recovery Process to make them aware with on the contents of BCP plan, prepare them for the activities to be performed during DR Drill/actual disaster and align them as per the duties and responsibilities of each party.

As stated in the SLA (Annexure to Volume- III) of this RFP, the Bidder shall design the CPP solution architecture for CPP Application and associated Services so as to ensure the following parameters:

Objective	Duration
RTO	**4 hours**
RPO	**15 minutes**

Bidder must consider the following criteria while designing Secondary Disaster Recovery Centre (DC-2):

1. Secondary Datacentre must be exact replica of the primary and should be no less in server capacity or storage.
2. Bidder hence must factor in a minimum planned and some unplanned number of hours for secondary datacentre (DC-2) and should factor that in commercials.
3. DC-1 should not require any configuration change for switchover to DC-2 in the event of disaster.
4. The CSP should have Datacentres at different physical locations in order to provide cloud Service offerings & Cloud Disaster recovery services, so as to mitigate the risk of both sites being affected by location-specific threats.
5. Once infrastructure at DC-2 is ready, the bidder should prepare detailed plan of replicating the configurations and data of the DC-1 to setup environment at DC-2.
6. The Infrastructure Design document must contain all relevant details of the DC-2 setup as well.

7. DR drill to test such switchover functionality shall be done periodically as per SLA. This would help to gauge the state of readiness of various other processes and procedure relating to business continuity and disaster recovery that may not get tested in a planned exercise.

DR Drills/Testing:

a. Business continuity plans must be tested. DR drills should be conducted on a six-monthly basis.
b. A test schedule should be drawn up for the business continuity plan. The schedule should indicate how and when each element of the plan would be tested.
c. The drill should include running all operations from Disaster Recovery Site for atleast 01 full working Day.
d. Formal approvals must be sought from IA&AD before the Drills are carried out.
e. Before DR drills, the timing diagrams clearly identifying resources at both ends (Disaster Recovery Site as well as Datacentre) should be in place.
f. The results and observations of these drills should be documented and placed before IA&AD.
g. Feedback from the tests should be used to update the plans.

The Bidder would communicate the results of the DR drills and any changes in the BCP to IA&AD after each test.

Additional features required as part of BCP setup are provided in RFP Vol-1 Annexure C.

6 Security Architecture

6.1 Guiding principles

For designing CPP Security Architecture, following Principles need to be adhered to:

1. Data Integrity: CPP Data must be correct, consistent and un-tampered.
2. Data Privacy and Confidentiality: Information need to be shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.
3. Non-repudability: CPP should ensure non-repudability of information in the system.
4. Secure by Design: Security has to be built into all stages and all aspects of architecture development, based on Zero-trust principle.

6.2 Security Requirements

The Bidder shall be responsible for meeting CPP project's comprehensive security requirements and 24*7*365 monitoring, analysis and management to ensure adequate security posture & security compliances. Bidder needs to ensure the compliance to the security requirement and monitoring of the threats/logs generated by various appliances. However, IA&AD reserves the right to further appoint an external agency to run Security Operation Center (SOC) for monitoring the adherence to security compliance requirements by Bidder. SOC in that case shall use security tools deployed by Bidder (at no cost to IA&AD) as part of the RFP.

6.2.1 Background Verification of Human Resources

1. Bidder has to ensure that all personnel deployed by or on behalf of Bidder for CPP project have undergone and passed background check. The background verification may be conducted by Bidder or an authentic third party. The Bidder would submit a certification in this regard to IA&AD within 10 days of deployment of resources.
2. Access controls: Bidder must ensure that the access rights of all employees, contractors and third-party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. Bidder will deploy process and technical control to implement the same.
3. All the resources deployed on the project will sign NDA with Bidder. Bidder would certify to IA&AD on quarterly basis that all personnel/resources deployed in the CPP project by Bidder or any other sub-contractor(s) on behalf of Bidder have signed the NDA with Bidder.
4. Bidder will ensure that qualified and competent Security resources with relevant experience are deployed as part of the team during the complete contract period i.e. during implementation and operation stage. The Personnel should have adequate experience, education and experience in the field of Information security. Information security experience (as per RFP vol-I) resource should be deployed as part of the team.

6.2.2 Security during Development and Operations phase

1. Bidder shall ensure that all the interfaces between various applications and users are encrypted using appropriate protocols (such as HTTPS, IPsec etc.), algorithm and key management

systems. Confidentiality and integrity of all the information flows transferred to and from the CPP system shall be secured from any tampering or leakage to unauthorized users.

2. Bidder to deploy a solution for Information Asset Register (IAR) that will capture and store details of all the digital assets and infrastructure deployed for CPP application, as per best practices and ITIL standards. Each asset should be trackable through a unique id throughout the entire project life cycle. The IAR register will also capture the physical assets along with serial number, model, make, location and other details to track the asset, wherever applicable. Any changes/updates made to any systems / sub systems / applications / infrastructure should be approved by IA&AD and updated in the IAR.
3. Bidder should have a CMDB (Configuration Management Database) to manage and track and audit the configurations of all assets deployed for CPP, include development artefacts.
4. Bidder will maintain separate environments between production and non-production environments to reduce the risks of unauthorized access or changes. No access to production systems / zone shall be permitted from Test and Development zone. No developers / developing team shall have access to production systems. No single DBA should be able to unilaterally make updates to tables / structures / rules / policies.
5. Bidder will provide for VPN solution for developers and O&M staff so that applications, code and infrastructure can be accessed from remote location. The solution and names of resources accessing the system via VPN will be prepared by Bidder and approved by IA&AD.
6. The systems, sub systems, databases and applications in CPP should have the functionality to automatically record all the administrator, user level activities including the failed attempts. All types of logging (audit, session, transaction, error logs, diagnostic logging) shall be enabled for databases. Bidder should size his compute and storage accordingly. The activities to be logged will be approved by IA&AD. Bidder shall protect logging facilities and log information against tampering and unauthorized access. Ownership and access to log server shall be exclusive from the system owners and should be clearly demonstrated by Bidder in the Segregation of Duties matrix.
7. Bidder will prepare the detail technical security solution design document to be submitted to IA&AD for review.
8. Bidder will define the secure coding guidelines and the same will be approved by the IA&AD.
9. Bidder shall incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts.

10. Bidder shall validate the data output from an application/module to ensure that the processing of stored information is correct and appropriate to the circumstances.
11. Bidder shall obtain information about technical vulnerabilities of information systems being used, evaluate the organization's exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
12. All systems / sub systems / applications that are acquired post go-live in context of CPP Project - whether COTS or developed by Bidder or procured by IA&AD or developed by third party from Bidder or IA&AD - shall also be assessed for security compliance prior to going into production.
13. All changes that go into systems / sub systems / applications for bug – fixes / improvement / feature enhancement / performance related / etc. shall also be assessed for security compliance prior to placing in production environment or go - live.
14. Segregation of Duties should be documented and monitored for access control and security requirements.

6.2.3 Access Control for Business users

CPP Applications shall involve authentication and authorization of the following two types of business users:

a) Pensioners – These will involve only basic level of authentication using user-id/password and 2FA. Role based access for pensioners is not envisaged. IA&AD envisages the authentication of Pensioners using a low-cost IDAM (LDAP, Custom solution etc.) solution only, as the number of Pensioners will be very high with very low concurrency.
b) Backoffice Users – This will involve authentication of users through user-id/password and 2FA. Role-based access of CPP Application and its services needs to be provisioned through IDAM. For back office users which are limited in number but will have wide variety of roles, an industry standard IDAM solution (with features listed in Annexure C) shall be required.

Following requirements should be addressed by the Bidder for provisioning of Access control in CPP Application.

1. Bidder will create a user profile database which will act as a master source to provide role-based access to the users.
2. The profile/user database will be managed centrally by the Cloud System administrator.

3. The solution should support multiple authentication methods such as Username / password, 2-factor authentication, digital certificate etc.
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The solution should have the functionality to provide authentication based on the role/privilege. The solution should have the capability to delegate the role privilege to another user, if required.
6. Single/multiple roles may be assigned to one user at the same time (e.g. additional charge of the post).
7. The Application should allow the user to switch/ toggle across roles.
8. The DMS capability should be able to demonstrate (provide an audit trail of) the details of user and activities performed by the users.
9. The Pension Back-office application must be an integrated solution. All the components of the application should support single sign-on and single logout. Application components may include BPM, BRM, DMS and KMS related functionalities, etc. The application experience for the end-user with respect to login, session management and logout should be seamless and synchronous. Bidder should evaluate the need of having an appropriate solution that allows only necessary access to the users based on their profile/role.
10. The session timeout for different components of CPP application would be synchronous and will be decided by IA&AD.
11. The user authentication to the CPP application would be based on Multi/2- Factor authentication.
12. All the user activities should be recorded in the system. The system should provide the feature to configure the logs as and when required.
13. The application shall allow only one session per user. The solution should have the option of blocking multiple sessions for the user.
14. The application should support role-based access control to enforce separation of duties.
15. The application should display the last login status (successful/unsuccessful time) to the user.
16. The Pensioner Portal application should be able to send a customized Account activation link (specific to each user) to the registered email id / mobile phone of the user. This link should be active for a specific duration of time for the user to activate the account. The user should be able to request for re-activation of this link.
17. The application should not store authentication credentials on client computers after a session terminates.

18. The CPP solution should be able to support password policies (complex password, change password in X days etc.) and allow configuration as per IA&AD requirements.
19. The CPP solution should be able to support OTP policies (format of OTP, expiry time, etc.) and allow configuration as per IA&AD requirements.
20. The solution should support automatic suspension of Pensioner accounts in case of prolonged non-usage. A warning (through Email and SMS) in this regard should be sent automatically before suspension. This is required for Pensioner portal only.
21. Administrator access – Access control solution shall
    a. manage administrator access to the components deployed such as operating system, network, database etc.
    b. ensure that direct access to servers / operating systems/ data bases is barred. Access to OS / middleware / sub- systems must be through a common access tool that logs all administrator activities.
22. The logs should be text-searchable based on key words entered in text.
23. The Application should be able to send the OTPs through SMS and Emails simultaneously. These OTPs must be active for a particular time duration only, as per IA&AD requirements.
24. Since OTPs are an essential component for allowing access to the users into CPP applications, it is imperative that SMS and Email services are provisioned with appropriate redundancy. Any downtime in these services will be tantamount to unavailability of the application. Appropriate SLAs in this regard will be applicable.
25. All logs of access to systems / sub-systems / applications must be kept for atleast 12 months. These logs shall be made available for forensics / fraud investigations whenever required.
26. Bidder shall ensure that the MIS reports generated from the system shall contain the name of the person generating the report along with date and timestamp in form of watermark.
27. Bidder will ensure that all the equipment, information or software shall not be taken off-site without prior authorization of IA&AD.

6.2.4 Security Compliance

1. Bidder will ensure that all infrastructure (viz. network, systems, sub-systems, firmware, etc.), middleware, and applications comply with the applicable IA&AD policies, IT Act, MeiTY and CERT-In (https://www.cert-in.org.in/) guidelines, standards, and reporting requirements during the entire contract period.

2. No unlicensed software, shareware, public domain software or pirated software will be used.
3. Bidder to ensure that any commercial software acquired, is used only in accordance with licensing agreements. Bidder to also ensure that any proprietary software is properly licensed before being installed in the CPP environment. IA&AD does not permit the usage of:
    a. Unlicensed commercial software
    b. Any Reversed Engineered -Cracked Software
4. Bidder should provide and reconcile all licenses with software installed/utilize. Bidder should maintain this inventory or audit of licenses in electronic and paper repository which shall be in the custody of IA&AD.
5. Bidder should also ensure that all updates, upgrades of all prescribed licenses software are obtained and installed on a regular basis. Updates, upgrades to be mandatorily taken for all security and network components.
6. Bidder shall execute all IT operations through detailed documented ITIL processes, procedures, SOPs, and work instructions including but not limited to Capacity Management, Availability Management, Problem Management, Identity and Access Management etc.
7. Compliance to Processes shall be measured as an SLA. Violations to processes discovered during internal / third party / security / independent audits would invite penalties as applicable.
8. Bidder shall also ensure the vulnerability assessments of all infrastructure (viz. network, systems, sub-systems, etc.), middleware, and applications as per defined SLA. Frequency of assessment shall be half yearly.
9. Bidder should perform the Penetration Testing for all internet facing systems / sub systems. Frequency of assessment shall be half-yearly till Phase 2 Go-Live and yearly for Post Go-Live period. However, in case if there are any major upgrades or changes in the application, an additional cycle of Penetration testing will be a pre-requisite before application is deployed in Production. IA&AD reserves the right to verify the security test results.
10. All **components of CPP System shall be audited by STQC/ CERT-In empanelled agency before CPP Phase-I Stage-1 Go-Live**. Bidder shall be responsible for successfully obtaining the certification and its submission to IA&AD. This will be a pre-requisite for all Go-live milestones in the life of the project, as described in RFP Vol-1.
11. Storage area/services used for CPP must be secured so that no other clients of the CSP are sharing the allocated storage.

12. Bidder also need to ensure the Patch management of all systems/ subsystems / network/ appliances/software as part of the security processes with OEM defined timelines for high, medium, low categories.
13. All services subscribed by the bidder through CSP should be fully secured and prepared environment. The bidder will take the full responsibility to ensure this.
14. Information systems must be assessed whenever there is a significant change to the system's security posture/architecture.
15. Bidder / CSP shall retain all data pertaining to CPP System till 1 (ONE) year after termination/expiry of contract or for the period specified by IA&AD, whichever is earlier.
16. Bidder / CSP shall protect all IA&AD data, equipment, etc., by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment will only be disclosed to authorized personnel. The CSP shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to IA&AD control, destroyed, or held as directed by the IA&AD. The CSP shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material. A declaration by the CSP/Bidder to this regard must be serviced to IA&AD based on IA&AD request.
17. IA&AD has the right to perform manual or automated audits, scans, reviews, or other inspections of the CSP's IT environment being used to provide or facilitate services for the IA&AD through an IA&AD designated third party auditor. CSP shall be responsible for the following privacy and security safeguards:
    a. CSP shall not publish or disclose in any manner, without the IA&AD's written consent, the details of any safeguards either designed or developed by the CSP under the Agreement or otherwise provided by the GoI & Government Department.
    a. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP. The CSP shall provide IA&AD records pertaining to technical capabilities, operations, and databases etc. within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
        i. Authenticated and unauthenticated operating system/network vulnerability scans

ii. Authenticated and unauthenticated web application vulnerability scans

iii. Authenticated and unauthenticated database application vulnerability scans

6.2.5 Information Security Incident Management

1. Bidder shall prepare the information security incident management process and seek approval from IA&AD before rolling out the application in production.
2. Bidder shall report and handle all the security incidents as per the timelines and action defined in the process document.
3. Bidder shall deploy appropriate technologies to detect and proactively response to security incident. Some of these technology solutions are Firewalls, Anti-APT, SIEM, IDS/IPS, HIPS, Anti-virus/Anti-Spam, etc., and are listed in this document. Bidder may propose additional tools to fulfil all the security requirements for this project.

6.2.6 Multi-layered Security Solution

1. Different layers of security in the hosting environments shall at a minimum implement the security toolset to provide Data Privacy and Data & Network Security by instating solutions such as Anti-Virus, Next Generation Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, Rights Management, SIEM, HSM, Integrated Vulnerability Assessment, SOC, Data Encryption, Certifications & Compliance, Authentication & Authorization, Auditing, etc.
2. The CPP Solution should have multiple security layers to prevent the infrastructure from any threats. The proposed solution should have different security zones as briefed below and all zones should have physically separate firewall, preferably from a different vendor. All firewall policies should be configured based on zone-based requirements.
    a. **Demilitarized Security Zone for Web server Farm (DMZ):** This security zone will host all servers that can be accessed from external world after due authentication and traffic filtering only. This zone shall host the APIs, CPP Web servers, etc.
    b. **Militarized security Zone for Database and Application server Farm (MZ):** This will be a secure Militarize Zone (MZ) to host all critical application, Data Base server, Storage etc. The Zone should not be accessible from Internet directly. All user traffic should be

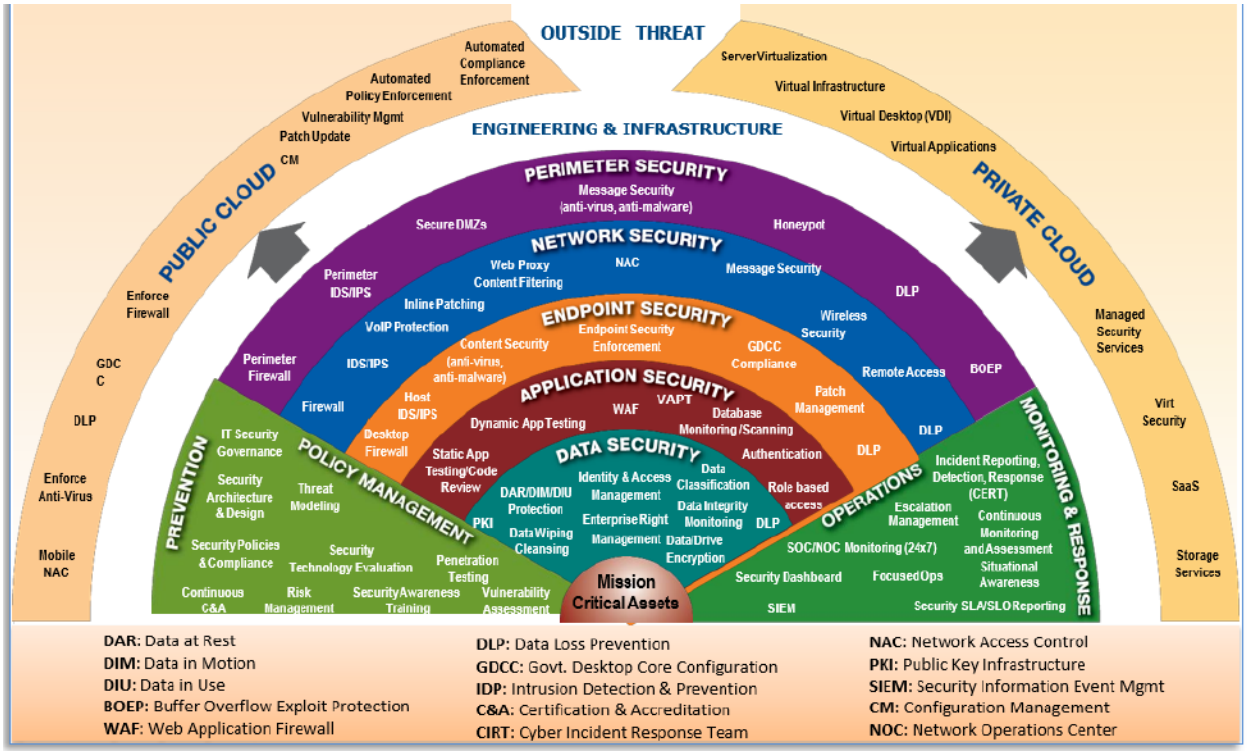
able to enter in this security zone via DMZ through controlled and monitored mechanisms as per CPP Security policy.

c. **Test and Development zone (TDZ):** This security zone will host all infrastructure required for testing, training, pre-prod setup and development environments. There should not be any access to Production zone from TDZ. These non-production environments should be created in a different VLAN, segregated from the production environment such that the users of the environments are in separate networks.

3. The Bidder shall be responsible for ensuring security of CPP application and infrastructure from any threats and vulnerabilities. The Bidder shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, event logging & correlation and vulnerability protection through implementation of proper patches and rules.
4. The Bidder shall deploy and update commercial anti-malware tools, investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.
5. The Bidder shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers.
6. Exchange of data between CPP and HRMS/IFMS systems at States may involve integration using various mechanisms such as API, Managed File Transfer, etc., depending on the capabilities of that respective system. However, the integration mechanisms at each of these states must be secured to ensure no data loss or theft during the data exchange.

6.3 Security Reference Model

IndEA Security Reference Model (SRM) is a framework for developing a comprehensive and rigorous method of describing the structure of the information security systems, policies and SoPs so that they align with the business strategies of the project. This model identifies the security controls to be applied at the **Data Layer, Application Layer, End Point Layer, Network Layer and the Perimeter Layer** as part of security architecture of an IT Application. It also provides the policies and procedures for Monitoring and Governance of Security framework during the Operations and Maintenance phases.



The different layers of CPP security architecture are aligned with IndEA SRM. Specific security requirements pertaining to CPP project have been detailed with each layer in the following section. Bidder should refer the BoM /BoQ for indicative list of security components/services. Bidder should design and deploy security solution as per the requirements of this RFP. The Bidder shall be solely responsible for any security breach/incident occurring during the life of the project. If the Bidder omits provisioning of any component(s)/ service(s) which is required to meet the project's robust security requirements, the Bidder will have to provision the same at no additional cost and time implications to IA&AD.

An indicative security reference model for CPP applications is detailed as follows:

1. Perimeter Security Layer
2. Network Security Layer
3. Application Security Layer
4. Data Security Layer
5. End point Security Layer (Refer 6.3.5 for exclusions)
6. Operations Management
7. Policy management

6.3.1 Perimeter Security Layer

The main functionalities at the Perimeter layer are to identify the appropriate security for every asset, application / service, and data. Based on the policies defined at the business layer, access to various assets, the appropriate configurations at various levels should be done.

Following components are required to be provisioned as part of CPP system:

a) Anti – APT - Proactive monitoring of scouting effort by hacker shall be done with Anti-APT using sand boxing.
b) Firewalls – Protects the infrastructure from unwanted or blacklisted intruders.
c) IPS – Provides Intrusion prevention at physical layer.
d) DDoS – Mitigates risk involving Denial of Services and Distributed Denial of Service attacks.
e) PAM – Securely manages the accounts and accessibility of users who have elevated permissions to critical infrastructure resources as per their authorized roles.
f) Content Filtering - Screen and exclude from access or availability, Web pages or e-mail that are deemed objectionable.
g) Message Security (anti-virus, anti-malware) – Appropriate anti-virus and anti-malwares should be identified and deployed. Policy regarding the same should be made to inform all the concerned.
h) Secure DMZ/MZ– Design the Datacentres network considering the sensitivity zones using Firewall.
i) Buffer Overflow Exploit Protection.

6.3.2 Network Security Layer

The Network layer would include the following security components/services provided as single/multiple component(s)/services by the Bidder for hosting at Cloud Datacentres:

a) Firewalls – to protect the infrastructure from unwanted or blacklisted intruders.

b) IPS – Intrusion prevention.

c) Application Security with user authentication.

d) SSL VPN: Bidder shall provide SSL based VPN access to the Bidder's team working on the CPP project to remotely access the cloud infrastructure.

e) URL filtering: Restrict content access by user.

f) SSL –All communication/data exchange (Data in transit) should happen over SSL.

6.3.3 Application layer

The security requirements mentioned below should be provided at the CPP application layer to secure the service / application and its data:

a) Web application firewall: Web Application Firewall must be provisioned to secure any threats coming through incoming web requests. Firewalls at application level should be given consideration to prevent attacks such as SQL injection, Cross Site Scripting (XSS), cross site request forgery etc.

b) HIPS Setup: All Application and Web Servers or any other middleware components shall have HIPS (Host Based Intrusion Prevention System) setup by Bidder.

c) DLP Setup: All servers shall have DLP (Data Loss Prevention system) setup by Bidder.

d) User Authentication: There should be a single sign-on authentication mechanism implemented in the CPP applications to provide access of the various application components/services via a single login. Two-factor authentication mechanisms must be built in the system for authenticating the users.

e) Role/ Rule based access: The users should be able to access CPP Application components/services/functionalities based on their assigned roles. A proper authorization policy and rules should be defined to prevent the unauthorized access to the various areas of the application.

f) SSO – All the components of the application should support single sign-on and single logout. The application experience for the end-user with respect to login, session management and logout should be seamless and synchronous.

g) Session Management – User session must be maintained securely until logout or timeout occurs for that user.

h) Files uploaded by end users must be verified at runtime for presence of any malicious content. The Application should be notified in case a malicious file is detected, so that appropriate error message can be displayed to the end-user.

i) Database monitoring: Monitoring the application, database servers for their uptime, threats which are being observed.

The Bidder is expected to carry out the following security and vulnerability related testing before every major release of the CPP application or major modification in the infrastructure/network:

a) Static testing and code review - Purpose of this type of testing is to identify the vulnerabilities without carrying out the actual execution of the code. Development or implementation team does this testing and provides the reports related to the same.

b) Dynamic application testing: Purpose of dynamic application testing is to determine the associated security vulnerabilities in the code by executing it. This helps to identify the security issues related to the complete production set-up including the exact version of the application and application stack.

c) Vulnerability assessment and Penetration testing: Objective of carrying out the VAPT is identification of vulnerabilities and possibilities of their exploitation. IA&AD reserves the right to verify the security test results. IA&AD reserves the right to perform Penetration Test. If IA&AD exercises this right, the Bidder shall allow IA&AD designated third party auditors to conduct and assist in carrying out testing activities.

6.3.3.1 API Security Layer

It is possible to attack or leak data in transit while calling the API and hence necessary measures must be undertaken to prevent their occurrence. The following care must be taken while designing API:

a) APIs / Services must comply with OWASP Top 10 guidelines.

b) Information required for routing or interpreting the contents of the packet should be part of header and should be appropriately tagged.

c) The body of the packet should be encrypted and should not be easily accessible. User's personal identity information should be part of the body of the packet and not the header.

d) Provide some default value for optional parameters/ tags.

e) Only necessary information should be taken from the user and unnecessary information exchange should be avoided.

f) API should be made available only on the secured channel.

g) Access to API should be provided only to the authorized users.

h) The data being consumed by the API from other sources must be verified for any malicious content.

i) Whenever data is exchanged between two servers, it should be done only after proper whitelisting of the IPs; requests should not be accepted from any other IPs.

Aadhaar APIs can be considered as a reference for designing secured APIs (Ref. https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf).

6.3.3.2 Mobile app Security

Following security requirements must be provisioned by the Bidder in the Mobile app:

a) All the data exchanged between Mobile App and the Datacentre must be secured using SSL Encryption.

b) The Mobile app should store only minimal data on the Mobile phone (which is mandatorily required to run the application) and in an encrypted format.

c) There should not be any unnecessary data or any sensitive user information like login details, password, personal information, case number, etc. stored on the mobile phone.

d) Mobile app should ask the user for allowing permissions to only those components of the mobile phone which are mandatorily required to execute that app and its functionalities.

e) Application should have capabilities of two-factor authentication to verify user identity at the time of user login.

f) The passwords of the user must follow the security policy as per CPP project's requirements.

g) User should be logged out of the app after a certain period of inactivity as per IA&AD requirements.

h) Mobile app should not have any code that attempts to get root access of the Mobile phone of the end-user.

i) Application should be provisioned to broadcast notifications to the existing app users about the release of an updated version of the app and prompt the user to update the app (from Android/Apple Playstore). Bidder shall be responsible to enlist the Mobile app on these playstores.

j) Mobile app should have tamper detection techniques built in it.

k) Malware in mobile phones often taps bugs and vulnerabilities within the design and source code of the mobile application. Appropriate prevention mechanisms must be built in the app.

l) Source code of the mobile app must be encrypted.

m) Mobile app should be backward compatible with up to N-2 versions of underlying mobile OS. Bidder shall make necessary changes to make the app compatible with future updates of mobile OS (N+2).

n) Mobile app and APIs must be audited for security by STQC/CERT-In empanelled vendors.

o) Follow platform specific Security best practices. Viz:

Android - https://developer.android.com/training/articles/security-tips.html

IOS: https://developer.apple.com/security/

p) Mobile app should comply with the latest version of OWASP guidelines published by OWASP Foundation. These guidelines can be found at the following location:

https://github.com/OWASP/owasp-mstg/releases

6.3.4 Data layer

Below functionalities should be provided for data layer:

a) Data needs to be secured / encrypted when at rest, at motion i.e. in transit or in use – Every piece of data irrespective of its sensitiveness need to be secured against the threats of unauthorized access, data corruption or complete data loss depending on the sensitivity and availability needs, methods should be applied to secure the data.

b) Data classification: Classification of data (Secret/ Top secret data as specified by IA&AD) shall be done by Bidder.

c) Identity and access management for data – The data should be accessible to only authorized persons, at appropriate time and only for the specified purpose.

d) Access Right Management – Access to data should be restricted by creating and applying a policy for every kind of data set. Data access policy will define the constraint for controlling the data access by its users. It will help in applying appropriate read, write controls over data elements.

e) Data Integrity monitoring – Mechanisms needs to be established by the Bidder to monitor integrity of all the Data stored within CPP system. Bidder must make all necessary provisions to enhance authenticity, reliability, and availability of data at Datacentres.

f) HIPS Setup: All data storage components shall have HIPS (Host based Intrusion prevention system) setup by Bidder.

g) Storage of Security encryption keys: Security Keys shall be stored in Hardware Security Module. Encrypted data of Aadhar number shall be stored in database (Aadhar Data Vault).

6.3.5 End-point Security layer

Endpoint security/management for Business Users is out of scope for this project, except for the Bidder's Development, Testing, and O&M teams that will be working on CPP project. For these users, the end-point security (including DLP) must be provided.

6.3.6 Security Operations – Monitoring

a) SOC monitoring: 24 x 7 Security Operations Centre shall be provisioned by Bidder at their premises.

b) Security dashboard: Security information and event management (SIEM) will be used to create and monitor security dashboard for performing security management.

c) Patch management: (Common to all layers) Installation of patch(es) released by OEM by Bidder's on all devices (Servers, VM'S, Appliances, etc.). Patch management plan and SoPs must be approved by IA&AD prior to Go-live.

d) Incident Reporting, Detection & Response (CERT): Monitoring and analysis of incidents by SOC Team shall be done by the Bidder. IA&AD must be notified about security incidents as per SLA.

e) Escalation management: Escalation matrix for notifying security incidents to IA&AD personnel shall be available with SOC team at a designated location/Tool.

f) Security SLA: Monitoring and reporting of security SLA shall be done by Bidder's team.

g) Continuous monitoring and Assessment: Security Audit by STQC/CERT-in empanelled agencies shall be undertaken by the Bidder's.

6.3.7 Security Policy Management - Prevention

a) IT Security Governance – Bidder shall create and submit Security Policy and Governance SoPs to IA&AD for approval. Bidder will be required to monitor and manage the IT security as per these policies and provide periodic reports pertaining to their compliances. Any deviation observed must be resolved by the Bidder within the stipulated timeframe.

b) Security Architecture & Design – Bidder must establish appropriate Information security controls in the CPP Design and Architecture for safeguarding it from various security threats as mentioned in this RFP.

Risk Management – A risk register shall be maintained by the Bidder for all the risks identified in the project along with their respective mitigation and contingency plans. Bidder shall continuously update the

risk register with risks occurred and any new risks that may arise during the project lifecycle. A copy of the risk register shall be made available to IA&AD at periodic intervals.

*****************The End****************

2021

Request for Proposal

Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

"Centralized Pension Processing System (CPP project)"

Volume – I

Annexure C

Technical Specifications & Compliance Requirements

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Contents

1 Overview

This document details the minimum required features and technical specifications of all the components of Application, Information, Infrastructure and Security Architecture. As preferred solution stays as cloud hosted and platform-as-a-service to the extent bidders can provide; this document should be referred for the specifications and features for each of the Technology components from software, hardware and managed services perspectives. The document should also be further referred for the indicative bill of material. Bidders can give justification for the departure from the indicative Bill of Material, but no compromise on the Quality of Services (QoS) will be accepted. This document should be treated as the checklist which bidders must provide answer to in the responses, in the same format, just filling the column of Yes / No and the remarks as applicable.

2 Guidelines for the Bidder

1. Bidder is mandated to provide availability/compliance status of the features/requirements for every component listed in this document as 'Y' or 'N'. The mentioned specifications should not be taken as an exhaustive list and is only an indicative list of requirements that gives a framework to the Bidder for preparing the solutions. Bidder can propose higher specification and justify its usage while presenting the design of the solution. Any additional component / functionality necessary to meet the solution requirements should be assessed and included by the Bidder as part of their proposed solution.
2. In case any feature/component is not readily/directly available (mentioned as 'N' in the Availability column), the bidder must explain why/how the non-availability/non-compliance of that component / feature would not impact the design/performance/requirements of the CPP Solution. Additionally, Bidder must provide alternative solution to fulfil that requirement / feature. The column titled 'Remarks' is to be used for this purpose.

3 General Checklist

The following checklist under this section should be treated over encompassing and across all areas of the solution.

3.1 Infrastructure Components:

S. No.	Features	Availability (Y/N)	Remarks
1.	Bidder shall assess the infrastructure requirements including Number of VMs, OS Instances, Storage, DC Networking, Security etc.) for hosting and maintaining all required applications / services as per the volumetrics specified in Vol-1 Annexure D. The Bidder shall provide the services as per the in conformance with the SLAs as described in the RFP.		
2.	The Bidder should ensure that all the services required for the completeness and functionality of the CPP solution, including but not limited to peripheral security, network, hosting, primary and secondary site management, required software, licenses, tools, services etc. has been provisioned according to the requirements of the CPP solution. IA&AD will not be responsible if the Bidder has not provisioned some components, sub-components, assemblies, and sub-assemblies as part of bill of material in the bid. The Bidder will have to provision the same to meet the solution requirements at no additional cost and time implications to the CPP project.		
3.	The Bidder should preferably use Open-Source Solution (Enterprise Edition/Support) for the system software. For COTS (Commercial-off-the-Shelf) products to be used, the same should be flagged and justified by the Bidder.		
4.	Either open-source (Enterprise Edition/Support) or COTS products, should be provided to IA&AD preferably in platform-as-a-service model. If some of the Technology components are not provided in PaaS model, the Bidder is		

S. No.	Features	Availability (Y/N)	Remarks
	encouraged to bundle it as PaaS to IA&AD. Adequate justification should be provided for such components that are not being provided in PaaS mode.		
5.	In case the bidder has to make a purchase of any license or support, it should be in the name of IA&AD. Also, Enterprise level support for system software should be provided for complete Project duration.		
6.	Bidder must not choose two different CSPs for Primary application hosting services and Disaster Recovery Services. Bidder further, should not make a hybrid cloud solution.		
7.	An additional backup (in addition to Disaster recovery) for application data, Backup/archived data/files must be kept at a distance of atleast 300 kms from either DC-1 or DC-2, even if it warrants engagement of a different CSP.		
8.	Bidder should avoid availing SaaS services from 3rd party service provider or any other CSP.		
9.	Bidder should ensure that the CSP is able to provide direct leased-line connections between Primary and Secondary Datacentres. Further, Bidder is to size the bandwidth requirements for the same and should ensure adequate provisioning through CSP.		
10.	CPP Solution and its services should be accessible via internet.		
11.	It is expected that the Bidder will provide an integrated solution, after due consideration to the compatibility issues between various components/services. If there is a problem with compatibility between components/services, the Bidder should replace the		

S. No.	Features	Availability (Y/N)	Remarks
	components/services with an equivalent or better component (that is acceptable to IA&AD) at no additional cost to IA&AD and without any project delays.		
12.	The Datacentres must be maintained ONLY at the declared hosting sites which should be communicated as part of the solution document.		
13.	All the applications would follow a three-tier / n-tier architecture with clear separation of database tier/layer from application and web layers.		
14.	If micro services-based architecture is being provided, Bidder should deploy Presentation, Business Logic and Database category of micro services on different VM's/Containers.		
15.	The Web layer for applications accessed via Internet shall be hosted in the DMZ zone; the Application layer should be hosted in the Militarized Zone.		
16.	The Database nodes should be in a MZ.		
17.	All management servers which are not directly accessible through the internet will be kept in MZ. Directory server, EMS, APM, SIEM, Different modules of Enterprise Management Servers (including network, server, database, ITSM tool, etc.), Single-Sign-On, access and identity management server, etc., will be a part of this MZ.		
18.	The solution should be able to discover all provisioned resources and provide details such as configuration items inventory, history of changes to such configuration items, snapshot of resource inventory at a single point in past, set-up of policies to track provision of resources		

S. No.	Features	Availability (Y/N)	Remarks
	within a client defined rulesets and auto-notifications each time a configuration change.		
19.	There will be separate VLANs/Subnets created for all Non-Production and Production environments to segregate their traffic across various environments. Appropriate firewall policies must be implemented to have further security between different zones.		
20.	The Bidder would size the solution for various Production and Non-Production Environments. High availability, to be provided as specified in the RFP for Production environment only.		
21.	Provide Audit logs of the account activity to enable security analysis, resource change tracking, and compliance auditing.		

3.2 Incident Response features:

S. No.	Features	Availability (Y/N)	Remarks
1.	The Bidder should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The Bidder must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures.		

S. No.	Features	Availability (Y/N)	Remarks
2.	The Bidder must bring in an ITSM tool through which the tickets (for incidents or other issues) can be logged automatically as well as manually.		
3.	The Bidder should have proper Standard Operating procedures defined and implemented, including chain of custody, required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customer and/or other external agencies engaged by customer shall be given the opportunity to participate in the investigation. Bidder is required to submit these SoPs with IA&AD as part of O&M preparation and must seek approvals from IA&AD.		
4.	A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Bidder is also expected to inform IA&AD if any weaknesses/risks are identified in the IA&AD's policies and procedures during the CPP project implementation and operations.		

3.3 Governance & Risk Assessment features

S. No.	Features	Availability (Y/N)	Remarks
1.	The Bidder should have organizational practices in place for policies, procedures and standards for application		

S. No.	Features	Availability (Y/N)	Remarks
	development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services.		
2.	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.		
3.	Solution proposed by Bidder shall have audit and compliance features which enables IA&AD System administrators to monitor the provisioned resources, performance, resource utilization, and security compliance.		
4.	Bidder should have security assessment mechanisms that should provide the following: a) Vulnerabilities assessment b) Penetration Testing c) Security policies including password policy, data storage access policy, etc.		
5.	The system should have ability to set up alarms for high resource usage (as defined in RFP) and the ability to define actions on triggering of those alarms (For example, ability to send an E-Mail when storage/ memory/CPU utilization has crossed x% or archive a storage section depending upon data type when it has crossed x% utilization)		
6.	Visibility into the performance and availability of the services being used, as well as alerts that are automatically triggered by changes in the health of those services.		
7.	The solution should provide a mechanism to provide details of all planned as well as unplanned downtime faced in the recent past (past 6 months at least).		

S. No.	Features	Availability (Y/N)	Remarks
8.	Bidder should provide report for monitoring RPO and RTO. The report should clearly show data replication process and any lag/ failure in data replication that should be notified through alerts to respective authorities.		
9.	The solution should be able to log all account and resource access into the log files (including the resources logging into the account using API call or root/admin users or other users logging into the system). These logs should be provided to IA&AD and/or agencies nominated by IA&AD for review.		

4 Cloud Service Provider (CSP) Checklist

The Bidder must engage a Cloud Service Provider (CSP) with the below mentioned criteria of CSP. Bidder must respond to each of the points on the checklist below. Bidder shall be responsible for compliance by the CSP for all of the following points.

S. No.	Features	Availability (Y/N)	Remarks
1.	CSP Datacentre should be minimum Tier III Certified. Copy of the Certification should be available from CSP.		
2.	The CSP should have minimum TWO Datacentres in India from where the MeitY empanelled Cloud Services are offered.		
3.	The CSP Datacentres from where the Cloud service are offered, should be located in India.		
4.	The CSP should have Datacentres at different physical locations in order to provide Cloud Datacentre Services & Cloud Disaster recovery services.		

S. No.	Features	Availability (Y/N)	Remarks
5.	Datacentre & cloud services offerings should have been successfully audited by STQC.		
6.	The CSP shall ensure that it always possesses a valid STQC audit certificate during the project duration.		
7.	Copy of the Letter of Empanelment to the CSP should be available clearly mentioning the Cloud Service Offerings and Cloud Deployment Models successfully empanelled with MeitY. The letter should also specify the Datacentre (s) facility from which the empanelled Cloud services can be offered to the government organizations.		
8.	The CSP must comply or meet any security requirements applicable to CSPs published (or to be published) by Ministry of Electronics Information and Technology (MeitY), Government of India RFP for Virtual Private Cloud or any standards body setup / recognized by Government of India from time to time and notified to the CSPs by MeitY as a mandatory standard.		
9.	The CSP must meet all the security requirements indicated in the IT Act 2000 the terms and conditions of the Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC.		
10.	CSPs should have the capability to transfer data back in-house or any other Cloud / physical environment as required by the IA&AD, either on demand or in case of contract or order termination for any reason		
11.	The Cloud Datacentres (including the Managed Services provided by the CSP) proposed for CPP project must comply with the following certifications and standards: 1. ISO 27001		

S. No.	Features	Availability (Y/N)	Remarks
	2. ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology 3. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in Virtual Public clouds 4. Privacy Standard: ISO 27018:2014 5. Quality Management System: ISO 9001:2015		
12.	CSP must share the Certification for SOC1, 2, 3		
13.	CSP should offer self-provisioning features (for VMs of different configurations, Storage, etc.)		
14.	CSP should provide billing available on pay-as-you-go basis (e.g. on hourly/daily/monthly/usage basis, etc.).		
15.	Auto-Scaling of resources (Compute or Storage) in real time should be parameterized and available in automated mode without human interventions.		
16.	CSP's cloud environment should provide flexibility to scale the environment vertically and horizontally: a. Vertically: Upscale/downscale the solution to higher configuration Virtual Machines (i.e. VMs/Containers with different combinations of CPU and Memory) b. Horizontally: Add more Virtual Machines of the same configuration to a load balanced pool.		
17.	CSP must provide default security features to protect application and data hosted on the cloud datacentres.		

S. No.	Features	Availability (Y/N)	Remarks
	Please mark the availability of the following features provided by the CSP in its Cloud Datacentres (put Y/N in the 'Availability' column against each of the features). a. Security against attacks like DoS / DDoS attacks, DNS attacks b. Perimeter security (using components such as Firewall, Anti-APT, Anti-malware, IPS) c. Private Subnets & Routing Bidder must provision any security component that is not available with the CSP from the list above.		
18.	CSP must log and maintain all necessary data points for any security incident analysis. For example, it should capture logs of all user activity and record information such as the source of incident trigger, time of incident, the source IP address, the request parameters, and the response elements returned by the cloud service.		
19.	CSP should offer monitoring Dashboard for all Cloud hosted services as single point of monitoring.		
20.	CSP must offer facility to manage resource allocation of different VMs/Container Services etc. taken as IAAS.		
21.	CSP must offer Cloud Infrastructure management services and is bundled along with the offering.		
22.	CSP must offer a documented and system driven process to allow any partner for configuration or administrative activities.		
23.	CSP must provide access to the unified Helpdesk and tool-based ticket logging and management system for incidents, changes and service requests.		

S. No.	Features	Availability (Y/N)	Remarks
24.	IT Helpdesk of the CSP must operates in 24x7 model and is able to provide Response and Resolution SLAs for Severity 1, Severity 2 and Severity 3 tickets.		
25.	CSP should Offer User authentication and authorization services on cloud which can scale up to millions of users, viz. LDAP, IDAM solution, etc. in a cost-effective model.		
26.	CSP must take the ownership of managed services software being used as genuine and complying to the licensing policy of the software OEM, for all components that it provides in PaaS model or if purchased from its marketplace.		
27.	CSP should be able to provide the cloud service offerings for a combination of the Deployment Models such as IaaS, PaaS, etc.		
28.	CSP must be able to offer multiple environments as mentioned in the RFP, clearly isolated from each other, as part of separate VLANs.		
29.	The CSP must support IP v4 and IP v6.		
30.	The CSP must provide managed services for provisioning and deployment of required compute infrastructure virtual machines, storage, security component, Backup, replication, DRM etc required to manage hosting and regular operations end-to-end.		
31.	The CSP should be responsible for provisioning and deployment of Internet connectivity with adequate Internet Bandwidth, including termination devices, for end users to access CPP application.		
32.	The CSP must provide required network infrastructure services such as firewall, Routers, Switches, VPC, ACLs and		

S. No.	Features	Availability (Y/N)	Remarks
	Load Balancer to ensure accessibility of the cloud services as per defined architecture.		
33.	The CSP should provide role based access for all users who need access to provision and manage Cloud services. CSP shall furnish regular reports on role-based access to IA&AD.		
34.	Admin access to cloud components must be secure and only be accessible from VPN.		
35.	The solution should provide the ability for IA&AD Administrators to access the cloud environment to view the metering, billing, and usage of services provisioned on cloud.		
36.	CSP must provide back-up-as-service as per the requirement. It will further provide the configurability for the backup schedules for data and the data of VMs as per RFP requirements.		
37.	CSP should provide the tools to monitor the performance of IT setup including the compute, memory, disk, IOs bandwidth, for provisioned services.		
38.	CSP should have the capability and is ready to provide customized reports/dashboard as required by IA&AD.		
39.	CSP must provide the support to provision and deploy the cloud services and also provides support to the Bidder and IA&AD authorized partners to deploy.		
40.	CSP should provide all required support to the IA&AD authorized 3rd party to perform the VA (vulnerabilities assessment) on application and infra which is deployed on cloud.		
41.	In case of exit or migration from the CSP, the CSP must provide all necessary handholding & transition support. For		

S. No.	Features	Availability (Y/N)	Remarks
	example, it provides support in migration of the VMs, data, content and any other assets to the new environment created by IA&AD or an agency on the behalf of IA&AD either on an alternative CSP or on-premises Datacentre.		
42.	The CSP should provide the mechanism for the bulk retrieval of all data, scripts, software, virtual machine images, and so forth to IA&AD for mirroring or copying to industry standard media.		
43.	The CSP should not use any proprietary data formats to enable portability. The format should be discussed and decided by IA&AD.		
44.	The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with IA&AD		
45.	The CSP should possess / create and manage all the documentation required by IA&AD for smooth transition including configuration documents kept up to date and all such documentation is provided to IA&AD on regular basis.		
46.	CSP shall protect all IA&AD data, equipment, etc., by treating the entire data as sensitive and will only disclose it to personnel authorized by IA&AD. The CSP shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to IA&AD control, destroyed, or held as directed by the IA&AD. The CSP shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of		

S. No.	Features	Availability (Y/N)	Remarks
	the material. A declaration by the CSP/Bidder to this regard must be serviced to IA&AD based on IA&AD request.		
47.	The CSP must ensure that IA&AD CPP application related data is not recoverable post agreement completion / exit process.		
48.	The CSP should implement a Change Management system that will facilitate and maintain all records pertaining to Changes made in the CPP System, in alignment with ITIL process.		
49.	The CSP should have the capability to provision High Availability of managed services as solutioned by Bidder.		
50.	CSP should provide Archival Storage for data to be archived as specified in Vol-1 Annexure B.		
51.	CSP must provide a managed API Gateway service for application to integrate with external systems via various protocols.		
52.	CSP should provide Monitoring Dashboard to monitoring the performance of CPU, Disk, Application, DB and other components.		
53.	CSP must provide information to IA&AD about the security incidents, threats and breaches occurring on the CPP related infrastructure components deployed in the CSP's datacentres.		

5 Managed Network and Security Services

Data and Application security is of paramount interest in the scope of the solution. Complying to the various layers of security Architecture, the Bidder must ensure availability of each of the security services on the Cloud Datacentre(s). This is to ensure that IA&AD data and application assets are safe in the Cloud.

S. No.	Features	Availability (Y/N)	Remarks
1.	The CSP should comply with the requirements of the Data Protection Act as and when published by the Government of India, within 1 year of publishing of the Act/rules.		
2.	All the IA&AD data, which is stored in cloud, should remain in datacentres hosted in India and it should not go outside India.		
3.	CSP should provide cloud services available from India location only.		
4.	CSP shall ensure that whenever IA&AD asks to delete any data from cloud then data should be deleted in all forms.		
5.	CSP shall have provision for (additionally) deploying the below security components as managed services to secure the hosting environments for IA&AD CPP application (specify Y / N in the 'Availability' column against each of the following components). 1) DDOS protection 2) Next Generation Firewall with capabilities to identify signature based and behavior-based anomalies 3) Anti-virus and HIPS (for virtual Machine) 4) Data Encryption at rest and in transit 5) SSL off-load/ Data protection 6) Web Application Firewall (WAF) 7) SIEM and Security Alerting and Reporting 8) Network Zoning 9) DNS 10) SSL VPN 11) Identity and Access Management 12) Load Balancer		

S. No.	Features	Availability (Y/N)	Remarks
	13) HSM 14) Privilege Access Management 15) Any Other Application and Infra Security components (as may be required)		
6.	Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control for each of the managed services.		
7.	Cloud Platform should be protected by fully managed Intrusion prevention system that provides network intrusion detection and prevention.		
8.	Cloud platform should provide security, threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc.		

6 Managed Database Services

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed Database solution must be present atleast once in the latest two published Magic Quadrant of Gartner's / Forrester Wave reports.		
2.	The Bidder shall provide either SQL and/or NO SQL / databases as managed service. The Database component chosen by the Bidder should be Enterprise Edition or have Enterprise Support agreements. Any additional expense to procure special licenses for Product support of the database(s), beyond what has		

S. No.	Features	Availability (Y/N)	Remarks
	been proposed by the Bidder in its bid, will be borne by the Bidder.		
3.	Database is available on Cloud infrastructure in High Availability (HA) mode both in Primary and Secondary Datacentre locations.		
4.	There is continuous replication of data between Primary and Secondary Datacentre locations at database level, however it could be block transfer.		
5.	Database services provided by the Bidder is able to exhibit high level of performance for all read and write operations.		
6.	The Bidder is able to provide all required activity logging at Database level for any audit or trouble shooting purposes.		
7.	All housekeeping activities such as log monitoring, performance parameters, resource allocation if the size is increased etc. are undertaken by the Bidder resources or the Bidder provides access to the console and support to the System Integrator to manage this.		
8.	Any issue discovered at Database response level that impacts the SLA levels of CPP Application needs to be furnished as the Root Cause Analysis and satisfactorily resolved with defined SLA.		
9.	Database proposed by the Bidder supports indexing and fast search using the index/key.		
10.	The Bidder provided Database would support role-based access to the data. All activity logs of Database access are recorded by the tool and are available for analysis in the event of suspicious activities.		

S. No.	Features	Availability (Y/N)	Remarks
11.	Configuration and Tuning of the Database provided by the Bidder is well supported by the Bidder resources.		
12.	There is auto provisioning of scaling the Database size as performance and size demands. This needs to be recorded and notified to the stakeholders.		
13.	Any change or upgradation in the version of the underlying Database is seamless to IA&AD and must not require any application level changes.		
14.	Read or Write access to the Database should be provided only through API / Data Access Layer calls. Database should provide functionality to restrict the access to database through the application only. It should provide feature to restrict users or DBA or any privileged user from accessing and/or modifying sensitive data through Query / Tools etc., using direct connection.		
15.	Any call to the database must be authenticated and only role-based access is granted.		
16.	Database managed services must include scheduled backup and retention as per IA&AD backup policy.		
17.	Database must have backup and recovery tool, which can support incremental backup. The tool should facilitate the partial recovery and full recovery.		
18.	Database solution should provide table and index level compression.		
19.	Database software must provide connectivity using native connectivity, JDBC, ODBC and connectivity to various technologies like .NET, ASP, Java etc.,		
20.	Database should have option for Automated/manual identification and tuning of high load and complex Query		

S. No.	Features	Availability (Y/N)	Remarks
	Statements. It provides details about dynamic tuning capability of the database depending on workload requirement, system resources etc		
21.	Database can have fault tolerance, parallel processing, linear scalability, mixed workload capabilities		
22.	Database should have ability to service concurrent multiple read and write requests and it can handle deadlock situations.		
Manageability of the Database			
23.	Database solution should have an ability to tune its performance parameters		
24.	Database should have capability to provide information/reports/dashboards to enable DB Performance manager to quickly identify potential problems and provide necessary resolutions.		
25.	Database Solution should also help to provide customizable reports with operational statistics of DB performance.		
26.	Database must provide lock mechanism and read consistency for concurrent transaction processing.		

7 DevOps Environment

Deployment of CPP applications/services/components or application changes etc. involving complex/layered architecture needs a seasoned deployment process and tools. It is recommended to use advanced capabilities such as DevOps which has capabilities of continuous integration and continuous deployment to reduce the time it takes for a change made in development environment to move to production after due testing and quality assessments.

The following features are required as part of DevOps solution, and could be offered as a single solution or comprising of multiple components:

S. No.	Features	Availability (Y/N)	Remarks
1.	Bidder should offer solution for DevOps consisting of: a. Coding – code development and review b. Repository - Configuration management tool for version management of source code and other project artefacts, code merging tool c. Building – Build / continuous integration tools, build status d. Testing – continuous testing tools for quick and timely feedback (Automated testing shall be preferred), Static code analysis, Vulnerability checks e. Packaging – artifact repository, application pre-deployment staging f. Releasing – change management, release approvals, release automation g. Configuring – infrastructure configuration and management		
2.	Solution must include Agile Planning tools for capturing the Product Backlog, defects list, etc. and tracking their progress over the development lifecycle across various Sprints and Releases.		
3.	Solution must maintain Version Control of all Production Artifacts: Both Dev and Ops should use version control and share the same single source of truth.		
4.	Solution must provision of deploying libraires and binaries into various Non-prod and Production		

S. No.	Features	Availability (Y/N)	Remarks
	environments directly from continuous integration (CI) tools.		

8 Business Process Management (BPM)

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed BPM solution must be present atleast once in the latest two published Magic Quadrant of Gartner's / Forrester Wave reports.		
2.	The BPM solution must be deployable on Cloud infrastructure and must be available as a Managed Service.		
3.	Should support multiple OS - Windows, Linux, UNIX OS		
4.	BPM Solution must support the following kinds of processes: a) Human Workflows b) Integration Workflows c) Decision Centric Workflows d) Event Based Workflows e) Case Management based Workflows		
5.	The escalation and notification mechanism in the BPM solution should provide integration with the following for sending automated notifications: a) E-Mail b) SMS		
6.	BPM Platform should have built in testing/simulation framework to test process end to end like Web forms, process flows, business rules while designing the processes		

S. No.	Features	Availability (Y/N)	Remarks
Process Modelling			
7.	Web based modelling tool must be capable of handling Business Process definitions		
8.	Modeler must be able to provide for modelling all business processes as per the requirements of the CPP application.		
9.	BPM Solution should have the capability to define a custom algorithm for task routing based on custom attributes.		
10.	The task routing capability in BPM should support default algorithms like round robin, least busy, most efficient etc.		
11.	BPM platform shall support easy to use design interface (e.g. drag and drop of workflow components) for designing / modifying process models by authorized users over web browser.		
12.	Tool should provide reusability for the connectors to integrate with other systems/applications.		
13.	Tool must provide abstraction of Process Definition from its Technical representation. A business user should be able to model the business process, separate from the technical aspects of the process. Specify number of sub-process levels which can be modelled in the modeler.		
14.	Business process can be of Person-to-Person, Person-to-Application or Application-to-Application type. The proposed tools should have capability to model all these types of processes.		
15.	Proposed solution tool should support modelling of sub- process with support of synchronous and		

S. No.	Features	Availability (Y/N)	Remarks
	asynchronous call		
16.	Proposed solution should provide an option of passing data from parent process to child process and returning of data from child process to parent process.		
17.	BPM platform should conform to industry workflow standards like **BPEL2.0/ BPMN2.0.**		
18.	BPM should not require any proprietary / other software to be installed on client machines to model or execute a business process.		
19.	Proposed solution should provide the Modeler to be used to define error handling within the process. It should provide an option of defining compensating activities or option of modelling exception flow.		
20.	It should enable designers to visually construct services, data transformations, BPEL orchestrations and integration to applications and back-end systems.		
21.	Proposed solution must support multi-tenancy feature, i.e. business processes, web pages etc. for different business entities such as departments/states should be configurable and stored segregated from one another, and should not be accessible by users of other departments/states.		
22.	Proposed solution should provide high reliability and support for long- lived processes that cross multiple applications by providing compensating transaction rollback and recovery.		
23.	Proposed solution should support modelling tool which has capability to execute the process end to end.		

S. No.	Features	Availability (Y/N)	Remarks
24.	Proposed solution should support modelling tool to store Business Processes to a common centralized repository for managing process deployments throughout the runtime environments—essential for program-wide governance.		
25.	Proposed solution should support modelling tool for tagging (assigning of tags) of artifacts / process parameters.		
26.	Proposed solution must support modelling tool which have the capability to have model UI collections / UI templates / views.		
27.	Proposed solution should support modelling tool support collaboration at design time i.e. multiple developers working on the same process at design time		
28.	Proposed solution should support the capability of versioning when the project is saved after changes.		
29.	The proposed modelling tool should provide a Process Server registry or equivalent with centralized tools to install and track deployed versions of multiple processes across various runtime server environments.		
30.	Web based modelling tool must be capable of integrating with Business Rules Engine and executing the rules as per the requirements of the Business processes.		
Execution			
31.	The proposed solution should have capability to provide runtime environment for the configured		

S. No.	Features	Availability (Y/N)	Remarks
	Business processes.		
32.	The proposed solution should allow the process engine to send/receive asynchronous as well as synchronous communication.		
33.	Tools supports execution of sub-process with support of synchronous and asynchronous call.		
34.	The proposed solution should have tool to schedule future events, steps, sub processes and process executions		
35.	The BPM solution should allow the running process instance to be stepped back to an older version, when needed, without having to stop the process instance.		
36.	The proposed solution must allow execution of a given/selected version of Business Process configuration in Production. Solution must also allow an upgraded configuration to become effective in execution environment on a given date.		
System Integration			
37.	BPM engine support integration with applications and systems that are participating in the process flow e.g. Databases, Messaging Middleware, DMS, Integration with other application/services thru APIs/Web services, etc.		
38.	BPM platform should allow integration with standard portals and allow single sign-on and single logout.		
Security			
39.	Solution should support the user authentication such as username/ password, One-time password before he/she can participate in process execution.		

S. No.	Features	Availability (Y/N)	Remarks
40.	Solution should support tool be integrated with user repositories like LDAP.		
Human Task			
41.	The proposed solution should handle human interaction with the process/BPM tool		
42.	The proposed solution should support intelligent routing capabilities. Tool support automatic routing of work to various participants		
43.	The proposed solution should offer possibility of allocating one task to multiple users		
44.	The proposed solution should have ability to set the priority of the task		
45.	The proposed solution should have an ability to easily remove or route the task out of the queue - rules based automatic and manual reassignment.		
User Interface Development			
46.	The tool support development of user interface - forms using a WYSIWYG editor.		
47.	The proposed solution should support integration with external data source(s) to pre-populate reference data.		
48.	The UI forms be easily integrated with the workflow.		
49.	The UI support access-based control to display data to authorized people.		
50.	The BPM Web Portal should provide support for inline task completion i.e. Completion of tasks directly from the task list without opening the task.		
51.	It should support/include UI based visualization tools e.g. dashboards, graphs, easy models of processes and webforms.		

S. No.	Features	Availability (Y/N)	Remarks
Process Monitoring			
52.	The proposed solution should support out of box tools available for monitoring and analysis of business processes.		
53.	The tool has ability to measure of timelines of tasks		
54.	The tool should have capability of tracing Process instance End to End		
55.	The proposed solution should support real time monitoring of process by user, managers or administrators. Availability of dynamically changing customizable dashboards		
56.	The proposed solution should support user define/configure parameters for which he/she can get reports		
57.	The proposed solution should support setting rules to respond to sets of events and pre-built KPIs		
58.	The proposed solution should support capability to business users to create adhoc reports dynamically based on some preset parameters		
59.	The proposed solution should provide reports that shows how many inflight tasks Broken down by status		
60.	The proposed solution should support tool have reports that shows Team member's individual statistics		
61.	The proposed solution should have support tool to generate reports that show tasks assigned/status to a particular team member.		
Case Management Capabilities			
62.	The proposed solution should support creation of		

S. No.	Features	Availability (Y/N)	Remarks
	Case activities for ad-hoc collaboration		
63.	The BPM platform should support the following. a) Case Details instance viewer b) Case Folder / Document viewer c) Case Work Items viewers d) Case Search e) Case task visibility via Dashboards ○ case documents ○ case stakeholders ○ case milestones ○ case events		
64.	The BPM solution should be able to support searching, viewing and updates to legacy Pensioners' data migrated from other IA&AD and State Government systems into CPP Database. Real-time integration with any external IA&AD / State applications for accessing legacy data from CPP is not envisaged.		

9 Business Rules Management (BRM)

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed BRM solution must be present atleast once in the latest two published Magic Quadrant of Gartner's / Forrester Wave reports.		
2.	The BRM solution must be deployable on Cloud infrastructure and must be available as a Managed Service.		
3.	Should support multiple OS - Windows, Linux, UNIX OS		

S. No.	Features	Availability (Y/N)	Remarks
4.	BRM solution and the configured rules should provide portability to other Co-Lo or Cloud hosting environments, with little or no effort.		
5.	BRM engine must allow seamless integration with BPM engine and CPP applications for execution of rules as per the requirements of the Business processes, preferably through Open standard API/Services. These API/Services pertaining to each rule should have clear Input and Output parameters defined for that rule.		
6.	BRM solution must provide easy to use web-based design editor that can be used by non-technical resources for creating and editing rules.		
7.	The design editor of the BRM solution shall provide drag and drop widgets (of rule components) for designing and modifying rulesets and rule models.		
8.	The solution must provide a natural language vocabulary / syntax to enable the non-technical authors to create and maintain the rules with little or no help from technical resources of the Bidder.		
9.	BRM editor must provide rule syntax checking capabilities to highlight syntax errors at the time of authoring the rules.		
10.	Proposed solution should provide the Modeler to be used to define error handling within the process. It should provide capability to handle exceptions during rule execution.		
11.	Modelling tool of the Proposed solution should support collaboration at design time i.e., multiple developers working on the same rulesets at design		

S. No.	Features	Availability (Y/N)	Remarks
	time.		
12.	The business rules created using the BRM solution should be configurable and must be separate from the application code. In other words, there should not be any need to re-build or re-deploy the application code / binaries in case of any modification to the rules.		
13.	The business rules for all States/Departments should be stored and managed from a common centralized repository and should be reusable across multiple applications. This is essential for program-wide governance of the rules.		
14.	Rules should provide various styles of defining rules such as, but not limited to, the following: • Computation rules • Work assignment rules • Delegation rules • Run time rules (vacation, adhoc process flow, etc.) • Approval rules • Escalation matrix • Applicability tables • Data Transformation		
15.	Business rule must support complex Decision Tables type of rules for deriving business decisions based on multiple conditions.		
16.	Proposed solution should support modelling and execution of nested rules.		
17.	Proposed solution should support modelling of orchestration / sequencing of multiple rules and their execution.		
18.	The proposed solution should have capability to		

S. No.	Features	Availability (Y/N)	Remarks
	provide runtime environment for the execution of the configured Business rules.		
19.	BRM solution must support multi-tenancy feature, i.e., business rules for different business entities such as States/Offices/Departments should be configurable and segregated from one another and should not be accessible by users of other States/Offices/Departments.		
20.	BRM solution must allow role-based creation and access to the rule components such as rulesets, decision tables, applicability tables, etc. for each State/Office/Department.		
21.	BRM solution must provide verification/maker-checker mechanisms for all rules created/modified before these can be published.		
22.	BRM solution must provide capability for version management, baselining and rollback of the rules, and maintain clean segregation between rules of different versions.		
23.	The proposed solution must allow execution of a given/selected version of Business Rules configuration in Production. Solution must allow an upgraded / configuration to become effective/ in execution environment on a given date or a downgraded (older) version to expire on a given date.		
24.	BRM solution should provide facility for concurrent deployment and execution of multiple rules / rulesets across multiple environments.		
25.	BRM Solution should have built in testing/simulation		

S. No.	Features	Availability (Y/N)	Remarks
	framework to test all types of business rules end to end while designing the processes.		
26.	The BRM solution must provide options of using multiple form of input sources (i.e., Excel spreadsheets, Database tables, CSV files, etc.) for testing and simulation of rules execution.		
27.	BRM should not require any proprietary / other software to be installed on client machines to model or execute a business rule.		
28.	The proposed BRM solution should provide capability for monitoring and analysing the business rules executed during a business process, activity, or transaction. Audit logs, Dashboard/customizable reports, etc. should be provided to the users based on their roles, for monitoring the details of the executed rule(s).		
29.	BRM solution must provide audit logs, dashboard (on console) / customizable reports of all rules executed during a business process or transaction.		
30.	The BRM solution should provide capability to compare changes between rules of different versions.		
31.	Solution should provide rule analysis support for finding anomalies from a set of rules such as redundant rules, duplicate or overlapping rules, gaps in decision tables, etc.		
32.	The solution should provide capability to search rule(s) based on rule properties and content. The BRE should have the capability to retrieve search results (of the rules) from the set of rules applicable to the user's		

S. No.	Features	Availability (Y/N)	Remarks
	State/department only, i.e., the search feature / results can be made restrictive as per user's access permissions.		
33.	BRM solution should be able to export and import rules in standard format (such as XML, CSV).		

10 Document Management Capability

An essential function of the CPP solution includes storing and managing scanned/digital documents related to the retirees or other stakeholders, such as digital signatures. The Bidders must note that the Document Management capability / Solution with respect to CPP is limited and hence should look for an apt solution that fulfils the following requirements accordingly. A checklist of Document Management Capability / Solution is provided below.

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed solution must have the capability of saving documents in file server and store metadata information of that document in database.		
2.	Inter-operability - The solution should support interface with other open-standard systems.		
3.	The proposed Solution should be deployable on Cloud infrastructure and should be available as a Managed service to IA&AD.		
4.	The Solution should have the capability of providing a pre-configured Watermark on the document(s) wherever required by the users.		
5.	Should be able to support the storage of digital records in the format of images and documents – viz., .tiff, jpeg, png, PDF, doc, xls, etc.		

S. No.	Features	Availability (Y/N)	Remarks
6.	The Solution should support categorization of documents in folders- subfolders just like windows interface. There should not be any limit on the number of folder and levels of sub folder.		
7.	The Solution must support versioning of documents with facility to write version comments		
8.	Should Support archival of documents (open ISO standard for long term archival of documents)		
9.	The Solution should provide facility to index folders, files and documents on user-defined indexes like Department, Ministry, file number, year, Document Category(-ies), etc.		
10.	The Solution should provide extensive search facility based on document meta-data/attributes or tags to retrieve documents or Folders/Files.		
11.	The Document management system capabilities shall support definition of Users, Groups and Roles relation in the system		
12.	The Solution shall support multiple levels of access permissions (Upload/Delete/Edit/ View/ Download) on Folders, documents and object level for the various Groups, Roles and Users.		
13.	The solution should provide multi-tenancy feature to segregate documents and their meta-data for each State/Department as may be required for CPP project.		
14.	The solution should have the capability to allow those documents that are required by all States/Departments to be stored at a common location accessible by all permitted users.		

S. No.	Features	Availability (Y/N)	Remarks
15.	The Solution shall provide LDAP support for integrating with directory services and shall support single sign on and single logout.		
16.	The Solution shall support Extensive Audit-trails at document, Folder and for highest levels for each action done by particular user with user name, date and time		
17.	The Solution should have "Out of the Box" integration/file-opening capability with popular office software e.g. MS Word, xls, ppt, PDF, etc. No third-party add-ons should be used to open these documents.		
18.	Must provide CMIS and REST API support. The proposed solution should not impose any OEM specific proprietary encryption while saving the images and binary documents at storage level.		
19.	The proposed solution should have the option to download a file to local PC/laptop/mobile devices. The user may upload the edited/updated version of the previously uploaded/downloaded document/file. The DMS Solution should have the capability to maintain multiple versions of a document (i.e. provide version control capability).		
20.	The proposed solution should have the option to download all/ multiple files as consolidated Zip/Rar file to local PC/laptop/mobile devices.		
21.	The Solution should provide capability to allow Digitally signing a document.		
22.	Embedding a QR code on the document as per CPP application requirements.		
23.	The solution must provide capability to have a user-		

S. No.	Features	Availability (Y/N)	Remarks
	defined Unique ID generated for a document.		

11 KMS Capability

The requirement for Knowledge management Solution for CPP application is limited to storing and managing scanned/digital documents such as published Government Rules, Orders, Acts, etc. pertaining to Pension processes. The KMS solution is expected to facilitate business users in directly uploading these documents (PDF, excel and other file formats) with associated meta-data and allow searching on this document repository.

User Access controls based on Documents are also expected to be enforced, e.g. Uttar Pradesh IA&AD pension office should be able to search documents associated with Uttar Pradesh only. CPP Application does not envisage requirements of any other KMS features such as Discussion forums, Wikipedia, Chats, Community of practice, etc. The purpose of KMS capabilities is limited to this extent.

The Bidder should propose an apt solution that fulfils the aforesaid requirements, i.e. Bidder may propose any KMS COTS solution or may use selected DMS solution (as described in section 10 of this document) to cater to KMS functional requirements or develop a customized solution.

12 Portal Capabilities

The CPP System shall have two different application URLs, i.e. two different web-based user interfaces – one for Pensioner Portal and another for CPP back office users. The pensioner portal would have a simple clean user interface which will allow public pensioners (large in number) to login, submit forms, view the application progress and status, log complaints, etc. (Refer FRS for details). There is only 1 user interface (design) for Pensioner Portal. On the other hand, the back-office application involves complex processes and multiple user roles and privileges. The UI for back-office application, thus, would have to be customized based on user roles. The portal would facilitate (after login) as a single platform for hosting dashboards, tasks, services associated with the user's role, etc. All the other CPP application components/services should be navigable through the Portal only. It is not expected that the UI design would be frequently changed (for both applications).

The Bidder should propose an apt solution that fulfils the aforesaid requirements, i.e. Bidder may propose any Portal COTS solution or may design develop a customized solution to fulfil the requirements.

The capabilities required to be supported for the Portal solution are listed below:

S. No.	Features	Availability (Y/N)	Remarks
1.	The portal solution should be deployable on a Cloud environment.		
2.	The web-based portal must have the capability of provisioning customizable web pages/forms, must support use of customized font colour and sizes, and display textual information as per IA&AD's specific requirements.		
3.	The portal must have the capability of customizing the Homepage with placeholders to display IA&AD icons, titles, etc.		
4.	The portal should integrate with Identity and Access management system to facilitate the User Login functionality, 2-factor authentication, etc.		
5.	The Portal should support integration with IDAM for customizing landing page as per the role of the logged-in user.		
6.	The landing page should be able to host customizable Dashboards, tasks, services associated with the user's role, etc. in a single web page.		
7.	The portal should allow switching the roles after login (in case two or more charges / designations are held by a single business user). Switching will involve changing the landing page associated with the new role.		
8.	The Dashboards hosted on the UI portal must support drill-down capabilities, pop-up etc. to display detailed information on the UI in real-time.		
9.	The portal must provide capabilities to the user to navigate and perform the assigned functionalities of the CPP Application as per the role of the logged-in user.		
10.	The portal must provide secure session management		

S. No.	Features	Availability (Y/N)	Remarks
	capabilities for the sessions maintained between the web browser and the back-end applications.		
11.	Portal UI must have the capability of integration with BPM (for executing workflows), open-standard APIs and services of CPP Applications and other 3rd party services associated with CPP project.		
12.	The web pages/forms of the portal must support search functionalities to filter required data-sets. The search results should be downloadable in multiple formats (such as excel, pdf, etc.)		
13.	The portal should be independent of form-factor and must provide a seamless mobile based experience to the end-users.		
14.	Portal UI should have seamless integration/hosting with selected reporting solution to facilitate generation of reports.		

13 Managed Enterprise Monitoring Services

The Monitoring system are meant to provide automated consolidated SLA reports for all the SLAs as mentioned in this RFP including real time status of various service levels achieved. The reports should be available through a centralized web access / dashboard and the access for this to be given to users as defined by IAAD.

All the solutions listed in this section should be deployable on Cloud infrastructure. In a cloud hosted environment such features are generally provided by the CSP and it is imperative on the Bidder to do a checklist with the CSP for all the areas of monitoring and if not then make additional provision in the solution to give a complete monitoring capability in the system.

The entire monitoring implementation shall be certified by the Bidder also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc. IAAD reserves the right to engage STQC/Other independent auditors for validating the deployment of monitoring facilities as per RFP requirements, especially

their capabilities for measuring and reporting SLAs & KPIs as defined in RFP. Bidder shall also provide in-depth training to the IAAD users (as per the SLA) on usage and operations of EMS solution.

13.1 Server Monitoring

S. No.	Features	Availability (Y/N)	Remarks
1.	Should offer service driven operations management of the IT environment hosted on the Cloud infrastructure to manage distributed, heterogeneous systems - Windows, UNIX & LINUX from a single management station.		
2.	Should provide a centralized point of control with out-of-the-box policy-based management for easy deployment (of EMS agents, if required) on the servers, operating systems, applications and services, for correlating and managing all the IT infrastructure components of a business service.		
3.	Should provide simplified service / process monitoring and have the capability for distributed management functions.		
4.	Should provide in built correlation to reduce the number of messages presented to the operators and to determine the root cause.		
5.	The system must have the capability of storing events / data locally.		
6.	System must be available in High availability and should support the backup server concept, which enables switching management responsibility from one management centre to another in case of system failure.		
7.	The System should have automated service discovery and should suggest corrective actions to enable busy IT		

S. No.	Features	Availability (Y/N)	Remarks
	personnel to focus on more strategic initiatives and manage business-critical application services from the end-user perspective, and to be immediately aware of the business impact of lower- level component failures or performance degradations		
8.	Complex dependencies between managed elements must be captured, allowing IT management staff to interpret lower-level data in terms of its importance to the higher-level service.		
9.	An advanced real-time status propagation mechanism in the Services view must allow IT management staff to immediately determine the impact of component failure on the overall application service. Problem-solving efforts can then be prioritized.		
10.	Alarms with customizable and standard message text, instruction text, operator / automatic actions / linked graphs, duplicate message suppression.		
11.	Should be configurable to suppress events at the agent or managed node level itself and be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.		
12.	The system should allow for enriching of messages with incremental information and should allow for customization of message attributes.		
13.	There should be a single agent on the managed node that provides the system performance data, and for event management, it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to		

S. No.	Features	Availability (Y/N)	Remarks
	add necessary annotations.		
14.	The system must support multiple built in discovery mechanisms for e.g.: Active Directory, Windows Browser, DNS with capability to discover and services discovery		
15.	The discovered services should be displayed automatically in consolidated IT management views in a single workbench Dashboard. This should portray the health of end-to-end IT services across IT infrastructure and domains.		
16.	Should provide console and a web browser interface that can be accessed from anywhere using industry-standard web browsers.		
17.	Each operator should be provided with user roles that should include operational service views enabling operators to quickly determine impact and root cause associated with events.		
18.	Highly scalable with ability to push deployment of agents and monitoring policies to a variety of heterogeneous platforms and applications running on cloud and enabling fast and controlled roll out and maintenance.		
19.	The EMS tool should have the capability to customize deployed agents for capturing required performance parameters, for which out-of-the-box capability is not available in the EMS tool.		
20.	The solution should have the capabilities to collect and analyze performance data from the operating system and installed applications and use historical patterns to evaluate against performance baselines.		

S. No.	Features	Availability (Y/N)	Remarks
21.	Agents on the managed node should be autonomous and can undertake automated corrective actions in isolation from the Management server. This will provide management by exception for only forwarding actionable events to the EMS Management server.		
22.	There should be secured communication between Management server and Managed nodes avoiding the need to open unsecure firewall ports.		
23.	The system must provide a manager-to-manager communication allowing management hierarchies to be established, such as several regional management centers linked to one central location, and to forward or escalate alerts depending on escalation rules. Escalation and forwarding must be fully automatic or handled through manual selection by Customer management staff.		
24.	The system may have its native database or capability to use external database for storing its data.		
25.	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS.		
26.	The system should have management polices to monitor and manage WMI, Performance, SNMP, Application, Log Files and Event logs and support automatic action in various forms like running a script to be taken on alerts from managed nodes.		
27.	The system should provide adequate help in capacity planning and provide trend analysis reports based on historical performance data.		

13.2 Application Performance Monitoring (including End User Monitoring and Diagnostics)

S. No.	Features	Availability (Y/N)	Remarks
1.	End to end Management of applications (based on technologies such as Java-J2EE/.NET, etc.) with deep-dive diagnostics		
2.	Determination of the root cause of performance issues whether inside the application in connected back-end systems or at the network layer.		
3.	Automatic monitoring of the web application environment and ability to monitor applications with a dashboard.		
4.	Dashboards should be easily customizable without any coding. Dashboards should be role-based so that business and IT stakeholders get the necessary visibility into the health of business and provide out-of-box KPIs that can be used to present different aspects of business service health.		
5.	Should have capability to monitor the third-party applications & services without any source code change requirements.		
6.	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnosis.		
7.	Monitoring of application performance based on transaction type.		
8.	It should proactively recognize and isolate transaction performance bottlenecks in applications along with intelligent alerts based on defined thresholds		
9.	It should deliver response time monitoring of both real-		

S. No.	Features	Availability (Y/N)	Remarks
	user and synthetic transactions		
10.	The system should offer a comprehensive end-to end transaction management solution for IT operations that may need to track transaction flows across heterogeneous applications/services.		
11.	Should drill down from slow, end-user transactions to the bottlenecked component, method or Query statement, helping to solve memory, exception and other common problems		
12.	Should automatically detect all components touched by a business process across layers and traces them with no user intervention		
13.	Should display the detailed Application processes/services that pinpoints the exact slow method within the entire application process/workflow/UI.		
14.	The proposed solution should report the performance of individual Database queries involved during business transactions		
15.	Data, reports and views from the monitoring solution should be reported via common dashboard views along with real user monitoring and infrastructure monitoring.		
16.	The solution must be able to scale to reflect performance and availability of additional services/applications without a significant increase in EMS solution		
17.	Should be able to provide the breakdown of the time spent on each component across presentation, business and database layers during a given transaction/process.		

S. No.	Features	Availability (Y/N)	Remarks
18.	The proposed solution should measure the end users' experiences in terms of response times based on transactions being processed in the system without the need to install agents on user desktops.		
19.	The proposed solution should measure the end users' experiences in terms of response times based on transactions being processed in the system without the need to install agents on user desktops.		
20.	The solution should act as a passive listener on the network thus inducing a near-zero overhead on the network and application layer.		
21.	The proposed system must be able to detect defects and anomalies impacting the users and report them in real-time, such as (but not limited to): • Slow Response Time • Low Throughput • Partial Response • Missing component within transaction		
22.	The proposed system must be able to provide the ability to create user groups based on application criteria or location and link user IDs to usernames and user groups.		
23.	The proposed system must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.		
24.	The proposed system must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web		

S. No.	Features	Availability (Y/N)	Remarks
	application.		
25.	The proposed system must be able to provide information related to root-cause for performance problems showing the most probable root- cause area.		
26.	The proposed solution should be capable of identifying the problem domain (browser, network or application) thereby it should monitor the browser side metrics and provide reports in real time for: • DOM Construction Time (ms) • Page Load Time (ms) • Previous page unload time (ms) • Browser Render Time (ms) • Page Roundtrip Time (ms) • Responses Per Interval (browser activity)		
27.	The proposed solution must be able to provide real time transaction health metrics and end user experience quality metrics.		
28.	The proposed solution must be able to provide the IAAD Officials/ IT team the flexibility to create artificial/synthetic users for executing business transactions and monitor real time application/service performance characteristics.		

13.3 Database Monitoring

S. No.	Features	Availability (Y/N)	Remarks
1.	The solution should monitor multiple database servers and multiple versions of each database proposed by		

S. No.	Features	Availability (Y/N)	Remarks
	Bidder as part of CPP System.		
2.	The Solution should provide statistics regarding the Response Time taken by the Queries during execution for performance Monitoring and optimization purposes.		
3.	Solution should perform Database Space Monitoring for both file group and transaction log.		
4.	Performance monitoring – Solution must capture DB Engine related performance parameters and send alerts at threshold values (Warning threshold, Critical threshold as well as file group/ log full).		
5.	The solution must support Agent monitoring to monitor query performance, failed jobs, long running jobs, etc.		
6.	The solution must be able to report & check for the last Full/Incremental database backup and last Transaction Log backup		
7.	The solution must monitor for Blocking (exceeding duration) and Deadlocks		
8.	The solution must be able to run DB monitoring commands/scripts to perform tests on the database and have the results put into the solution as performance data and / or alarms.		
9.	Inclusion of Query statements within the Solution should be a standard "easy-to-use" function achieved without programmatic intervention.		
10.	The solution should support auto - discovery of database instances.		
11.	The solution should provide database monitoring for execution of transaction running in the system and should provide information of a particular point/range of		

S. No.	Features	Availability (Y/N)	Remarks
	time.		
12.	The solution must have the capability to provide Database statistics collated for entities present in the database. Solution should also have the capability to display statistics on the dashboards segregated for each respective entity within the Database. .		

13.4 Dashboard & Centralized Reporting

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed solution must provide built in system for correlating events, creating alerts based on it and enforcing automated action policies.		
2.	Proposed Dashboard solution should have Out-of-the-Box connectors/ probes to integrate with the EMS solutions proposed by the Bidder for CPP and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and Network Monitoring System (NMS) solutions. In case the Dashboard solution does not integrate with any of the proposed systems/solutions/services, the Bidder shall provide alternative mechanism of Dashboard integration at no extra cost to IA&AD.		
3.	The solution should have cross-domain reporting module which allows to make future decisions by seeing behaviour patterns by service, application, operating system, virtualization platform/technology like hypervisor, middleware, database, etc.		
4.	The system should provide ability of correlation rules,		

S. No.	Features	Availability (Y/N)	Remarks
	tools, and KPIs across the environment.		
5.	The system shall allow administrators to create new Event Correlation rules and indicating which event is the cause and which are the symptoms.		
6.	When combination of many similar events occurs in the monitored environment, the system must be able to automatically collate them into a single cause and symptom.		
7.	Tool should provide complete view of application and Cloud infrastructure health across the environment into a central console.		
8.	Should provide reports that can provide IT service quality levels, such as application response times and server resource consumption on the same pane.		
9.	Reports can be scheduled to publish automatically or they can be produced on demand.		
10.	Reports can be applied to all systems, to a group of systems, to a customer group of systems, or to a single system.		
11.	Reports can be published in HTML, PDF, Word, and Excel formats.		
12.	Should have the capability to send reports via E-Mail from the user interface.		
13.	Tool should provide a library of out-of-the-box reports in the context of business services.		
14.	Tool should provide the capability to provide the variety of reports using data sources such — Generic .csv files, and Databases supporting JDBC. Should also be included to pull data and create reports from such data.		

S. No.	Features	Availability (Y/N)	Remarks
15.	Tool should allow to configure/ define change/ maintenance window for monitored infrastructure		
16.	The tool should also have a web-based user interface with user authentication facility to allow management of events and access of reports from anywhere 24 X 7.		

13.5 SLA Monitoring & Reporting

S. No.	Features	Availability (Y/N)	Remarks
1.	The solution must be able to monitor all types of cloud service offerings (E.g., PaaS, IaaS, etc.)		
2.	The solution should have capability to configure, capture, measure & report service level parameters at specified frequency as mentioned for each SLA in the RFP.		
3.	The solution should have the capability to integrate with all Component/Services deployed in the CPP System for capturing and monitoring SLA related data of all these components.		
4.	The solution should provide a flexible framework for configuring and managing Service level templates including complex Service Definitions, Service Level Targets and other Performance indicators.		
5.	The solution should have the capability to monitor, collect metrics and report performance of all the configured SLAs pertaining to the components/services deployed in CPP System such as VM's, Network, Replication systems, Servers, Applications, Third-party components/services, etc. in real-time.		

S. No.	Features	Availability (Y/N)	Remarks
6.	The solution must be able to send Alert notifications (E-Mail/SMS) to various stakeholders as configured in the solution for each SLA.		
7.	The solution must be able to store and display service level data for at least 1 year.		
8.	The solution must be able to provide SLA reports, along with dashboards and charts, and allow these reports to be exported in formats such as .csv, excel, pdf, etc.).		
9.	The reporting format of the solution should have provision to customize data into a standard format for the whole environment (i.e., including reports of Third-party components/services) as required by SLAs defined in this RFP		
10.	Audit Trails: The solution should provide audit trails for the SLA related data captured by the solution, for further verifications and analysis.		
11.	The solution should have Dashboards for depicting the various SLA measurements along with comparative analysis of the SLAs over a period of time.		

14 Disaster Recovery services / Business Continuity Planning

The RFP requires an automatic failover to take place between the two Datacentres in case of a disaster and the application should be made available as defined under RTO and RPO. Bidder may choose the architecture (Active-Active or Active-Passive as per proposed CSP's offering) between the DC-1 and DC-2 Datacentres through which the Disaster recovery for application and application data will be ensured. Bidder is expected to employ appropriate tools to manage the Disaster recovery as per the defined SLAs.

S. No.	Features	Availability (Y/N)	Remarks
1.	CPP solution should be architected to run on one Datacentre facility to provide business continuity as per defined RPO and RTO and SLAs.		
2.	In case of disaster at Primary Datacentre (DC-1) site (within the defined RTOs and RPOs), the Secondary Datacentre (DC-2) site should be available (with its data) on-demand basis, wherein 100% of the services of DC-1 would run from DC-2 site (after the RTO time and with the RPO level). Once the DC-1 is restored, fallback to DC-1 must happen automatically.		
3.	Bidder should size solution as per defined RPO and RTO and SLA.		
4.	Solution should provide automatic switchover of individual applications/services/ components apart from the entire system in case of a disaster. Solution should have the capability to automatically switchback the applications/services/ components to Primary Datacentre as and when it is available again.		
5.	Solution should have the capability to monitor both Cloud based Datacentres for the availability of applications/ services/components and should be hosted on Cloud infrastructure.		
6.	In case of failure, automated/manual processes should resume services from DC-2 site. The Bidder would ensure that adequate bandwidth between the Datacentre Facilities to provide business continuity.		
7.	In case of failover to Secondary Datacentre (DC-2) site (once disaster is declared), the SLA performance parameters would not be applicable for RTO period. The		

S. No.	Features	Availability (Y/N)	Remarks
	DC-2 Site should take over the operations within the RTO period. The details of SLA performance parameters, which could be relaxed and the extent of such relaxation during the operations form the DC-2 Site would be decided by IA&AD after first DR drill. IA&AD reserves the right to modify/amend such relaxations. The Bidder has to ensure that the operations are switched back from DC-2 to DC-1 site promptly.		
8.	Solution shall provide a single view of all the applications/services/ components of both the Datacentres.		
9.	Solution shall provide reports pertaining to Failover and Recovery of application and services, and other migration activities.		

15 Reporting Capability

Reporting is an important function of the CPP solution that provides insights into the various Operational aspects and other performance indicators of the application and its infrastructure components. The Bidders must note that the requirements of reports in CPP are limited, and hence should look for an apt solution that fulfils the following requirements accordingly. IA&AD does not visualize use of a complex BI tool/solution for implementing Reporting capability in CPP.

A checklist of Reporting Capability / Solution is provided below.

S. No.	Features	Availability (Y/N)	Remarks
1.	It should support creation of custom reports through an easy-to-use, self-help web-based interface.		

S. No.	Features	Availability (Y/N)	Remarks
2.	The reporting solution should be deployable on Cloud infrastructure.		
3.	Interactive report viewer that allows the users to perform activities on the reports' tables and charts such as sorting, filtering, conditional formatting, moving/hiding columns, string search, zoom in/out, and allow these changes to be saved for using in future.		
4.	Ability to present Data textually as well as graphically using Dashboards, Graphs, Charts and Tables.		
5.	The solution must allow users to apply Watermarks to reports while downloading.		
6.	Ability to export Various common formats of reports such as .xls, .csv, XML, HTML, PDF, etc.		
7.	It should support auto-generation of reports through Scheduling process.		
8.	The Solution should support drilling-down on summary data displayed in reports/dashboards to automatically show the detail in real-time.		
9.	It should support restricting user's access to generate, change & view the reports and queries in the system. Appropriate access control mechanisms should be defined in the solution to allow restricted access to the reports and the reports data based on each user's roles, responsibilities, and State/Department.		
10.	The solution must have the capability to restrict the generation of reports based on the access profile (record-based permissions etc.) of the user generating the Report(s).		
11.	Solution should support Integration with Portal UI		

S. No.	Features	Availability (Y/N)	Remarks
	Dashboard based on pre-built queries, as per User profiles.		
12.	It should support Automated and secure logging and maintaining audit trail of reports generated, reports accessed, and reports changed, e.g., User details, Date and Time stamp, query/report name, etc.		
13.	The solution should support performing calculations/computations while generating the reports.		
14.	It should provide a platform for advanced users to apply various queries on the CPP databases to fetch specific results.		
15.	Business users should be able to generate any custom report based on Meta Data elements of the documents available in the Application and Business process stages.		
16.	Solution should support reporting of summary statistics (with drill down) for Business Service Levels which are at breach/ near breach levels.		

16 Contact Centre Solution for Service Desk

The proposed solution shall provide a system to automate call-based and chat based real-time interactive support that will be used by CPP users and Pensioners to report their issues and grievances over phone/chat. This solution will then be used by the back-office/functional/technical helpdesk support staff to provide resolution to those incoming calls/chat requests.

The contact centre personnel will be IA&AD employees and shall be stationed at different geographical locations in different states and offices. All the personnel shall login into the same Contact centre solution and perform their activities.

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed solution shall provide a web-based service support system to automate call-based and chat based real-time interactive support.		
2.	The proposed Service Desk solution must be hosted on a highly secure Cloud Infrastructure, which must be certified for ISO27001, ISO 27017, ISO27018 as well as SOC 1,2,3.		
3.	The proposed Service Desk should have features of User authentication, authorization, and privilege management.		
4.	The proposed solution shall support tracking of SLA (service level agreements) for call requests within the service desk through service types (that define response/resolution time)		
5.	The proposed solution shall provide standards-based / API-based integration mechanisms that allows this solution to register incidents in an Incident Management (ITSM) tool and provide information about the status of the incidents to the end user. The Incident management (ITSM) solution may be hosted on a different Cloud infrastructure.		
6.	The proposed solution should be able to integrate with CPP application/services to automatically fetch the basic details of the caller (such as Name, department, grade, E-Mail, etc.) and auto-populate / capture those user details in the Contact centre against the incoming call. These user details also need to be captured automatically while logging the ticket.		
7.	The proposed solution should provide facility for call recording and archiving of the recordings. These call recordings should be available to L2/L3 personnel.		
8.	The solution should allow provisioning of custom fields for		

S. No.	Features	Availability (Y/N)	Remarks
	a call to allow the Helpdesk agent to capture other custom information about the call such as Issue Description, logged Ticket no., call recording URLs, etc.		
9.	The solution should provide the capability to search previously saved call details, call recordings, previously saved tickets from same call (to be automatically populated) to help agent resolve the current issue at hand faster.		
10.	The solution should provide the capability to integrate with E-mail and SMS services.		
11.	The solution should provide personalized and role-based dashboards and out of the box reports as well as custom reports.		
12.	The Contact centre should be able to automatically route the calls to the preferred agent based on the extension selected.		

17 ITSM (Helpdesk) Solution

There is a need of an Incident, Change and Service request management tool in the solution scope of CPP, that is required for responding to and resolving the queries and issues from the consumers of the system, i.e the back-office Service Desk / (L1, L2, L3) IT Support users to attend to the incidents, manage service requests and changes. Following checklist can be referred by the Bidder while proposing the ITSM solution.

Note: In case offered EMS Tool provides all the Helpdesk functionalities stated above, then Helpdesk can be offered as part of EMS. The Bidder should explicitly mention this in his bid.

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed ITSM solution must be a web-based solution		

S. No.	Features	Availability (Y/N)	Remarks
	deployable on Cloud infrastructure and must be available as a Managed Service to IA&AD.		
2.	The ITSM solution must automate and manage end-to-end lifecycle management for the incident, problem, change, service request, knowledge management (pertaining to ITSM), interactive support, self-service and Asset management.		
3.	Real-time progress updates - The proposed solution should help the service agents to check the progress of their individual KPIs or status of any incident/ticket in real time through dashboards and reports.		
4.	SLA Management: The proposed solution shall support tracking of SLA (service level agreements) for all incidents/requests logged within the solution for different service types (based on pre-defined response/resolution time)		
5.	SLA Measurement: The Proposed solution shall provide SLA (Response SLA and Resolution SLA) at individual Ticket Level. The SLA measurements should be dynamic in nature and should clearly highlight the tickets for which the SLA breach has already occurred or are nearing SLA breach.		
6.	Application Integration: The proposed solution shall provide open standards-based integration mechanisms (e.g. REST API, Web services, etc.) that allow infrastructure management solutions to automatically register incidents.		
7.	Contact Centre Integration: The proposed solution shall provide open standards-based		

S. No.	Features	Availability (Y/N)	Remarks
	integration mechanisms (e.g. REST API, Web services, etc.) that allow Contact Centre solutions to register incidents.		
8.	Incident Categorization: The proposed solution shall provide multi-level ticket category classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, Business Urgency levels and Business impact levels.		
9.	Auto allocation of incidents: The proposed solution shall provide the flexibility of automated incident assignment based on metrics such as analyst workload, category, location, repetitiveness of the incidents and standard incident queries, etc.		
10.	Segregation of Users and Incidents - ITSM tool must allow for creation of multiple environments/zones within its deployed instance to allow segregation of the Users and incidents across these zones and maintain authorized access of each zone to its assigned users only.		
11.	Auto-populating the ticket attributes based on pre-configured incident categories - The proposed solution should allow configuration of all necessary attributes of a particular category / nature of incident. At the time of logging a new ticket, when the helpdesk user selects a particular category of incident, the other attributes for that incident should be auto populated based on the pre-configured attributes.		
12.	Problem Management: The proposed solution shall provide problem management module for recording problem and its work		

S. No.	Features	Availability (Y/N)	Remarks
	around / resolution. The solution must be able to relate and link a given problem to specific incidents logged in the tool.		
13.	Problem Management – Bulk Closure of tickets: The proposed solution should provide features for closing multiple similar incidents through a single problem at a single click.		
14.	Search Capability: The solution should provide the capability to search previously saved service request, incidents, and problems.		
15.	Similar Ticket Search: The solution should offer similar ticket search facility that should result only list of service requests, incidents, and problems having the same Classification.		
16.	E-Mail Integration: The solution should provide the capability to integrate with E-Mail and SMS services, so that the solution can send outbound notification E-Mails / SMSes to the users. These notifications may be triggered at various stages of lifecycle of a ticket (e.g., logging of the ticket, resolution, closure, re-open, etc.). These notifications should also be reflected in the communication log as a part of the ticket record.		
17.	Flexible Reporting/Report Configurator: The service desk users should be able to define custom reports through configurations according to their business needs.		
18.	Auto-Capture of Activity Log for Audit Purpose: The proposed solution to provide automated capture of activity log with date and time stamp, action taken with		

S. No.	Features	Availability (Y/N)	Remarks
	action details, and user details for all incidents. These would be used for audit purpose.		
19.	Customer Feedback at Ticket Closure: The proposed solution to provide capturing customer feedback after resolution of every tickets. Based on feedback received from the end user, the helpdesk user can close the tickets along with given feedback or reopen the tickets if the user is not satisfied with the resolution.		
20.	The proposed solution should provide various service management graphical and data based reports such as productivity reports, compliance reports, Satisfaction Reports, etc. Reporting automation features should be available for automated daily status reports.		
21.	Change Management: The proposed solution to provide an end-to-end process for change request management. It should include fields to capture business requirement Definition, approval process workflow and change request execution process steps.		
22.	Task Management: The proposed solution to provide multiple task management features against a particular problem or change request or service request.		
23.	Asset Management: The proposed solution to provide Asset Management and Configuration Management database features against incident, problem, change or service request. Provision for maintaining Configuration Items (CI) should be made available.		

S. No.	Features	Availability (Y/N)	Remarks
24.	Escalation: Escalation features where agents can route incidents/business related query and difficult tickets to the higher-ups of SI and IA&AD officials as per the Escalation matrix.		
25.	Auto-Closure of Tickets: The proposed solution to provide auto-closure functionality for resolved tickets that are not closed by customers. Auto-closure rules should be configurable and based on business inputs.		
26.	Auto-Closure of Tickets generated by EMS: The tickets generated by EMS should be automatically closed for all events if the service level breach/issue resolves back to permissible service level within the time limits as defined in the SLA. The ITSM solution must provide the capability to report such auto-closed tickets separately.		

18 Infrastructure Services

All the Infrastructure components/services/solutions listed in this section and/or provided by the Bidder in their proposal should be deployable on Cloud infrastructure. The Bidder must ensure that it establishes all the security controls and infrastructure setup necessary to comply with the requirements and adhere to the SLAs and KPIs for the CPP project as per the RFP, even if it entails setting up of some additional components. Bidder shall be liable for procuring/provisioning of any component/solution that may be additionally required during the life of the project if any deficiencies are found w.r.t. RFP requirements and/or achieving SLA KPIs.

A checklist of features pertaining to the Infrastructure Components / Solution envisaged for CPP project are listed in this section.

18.1 VMs/Container services

S. No.	Features	Availability (Y/N)	Remarks
1.	Should provide bare-metal architecture of a robust virtualization layer of a ready to use virtual machine / containerized services along with an operating system directly on the server hardware.		
2.	Should provide CPU virtualization. Provide the ability to Run many operating systems and applications encapsulated inside virtual machines		
3.	VM/Container services should be capable of hosting Operating systems such as Windows, Linux, Unix, etc.		
4.	The solution should be scalable. It must have provision to add/increase virtual CPU, RAM & Disk to a running virtual machine without having to suspend/ shutdown/ restart.		
5.	VM/Container services should support live virtual machine migration in event of failure of any running Virtual machine/(s).		

18.2 Server Operating System

S. No.	Features	Availability (Y/N)	Remarks
1.	Offered OS should be Enterprise/ Datacentre edition.		
2.	The Server operating system should support the essential network services like Directory Services (LDAP), DNS, DHCP, Radius, Web Server, Application server, Cluster services (High Availability and Fail over Support), Load Balancer, with virtualization support.		
3.	OS should conform to TCP/IP communications standards interface based on Internet Standards. The OS should		

S. No.	Features	Availability (Y/N)	Remarks
	support protocols / services / standards including, but not limited to, IPv4, IPv6, ICMP, IP Multicasting, User Datagram Protocol, SNMP, HTTP, SSL with FIPS certification, Domain Name Service, Telnet, SFTP, NFS, CIFS, SMB, Bootstrap Protocol, DHCP, Network Time Protocol, etc.		
4.	OEM / CSP providing support for OS should be available 24X7 via E-Mail, helpdesk and contact centres.		
5.	Any Open-source OS proposed by the Bidder must be procured with an Enterprise support.		

18.3 Web Server

S. No.	Features	Availability (Y/N)	Remarks
1.	The solution must support deployment of one or more web applications and web services with request queuing and caching		
2.	Should support load balancing		
3.	Should have the ability to store web server configuration data in configuration files.		
4.	Should support web-based administration console for deploying web applications and making relevant configurations.		
5.	Should Support for Web Distributed Authoring and Versioning and Web Folders		
6.	Should support integration with digital certificate services		
7.	Web server should be deployable on Cloud infrastructure.		
8.	Must Support industry standard mechanisms for		

S. No.	Features	Availability (Y/N)	Remarks
	Authentication with LDAP, Kerberos, and RSA tokens.		
9.	Ability to distribute HTTP client requests across multiple web containers.		

18.4 Application Server

S. No.	Features	Availability (Y/N)	Remarks
1.	Application server solution must support deployment of one or more applications and services on Cloud infrastructure.		
2.	Must be completely compliant with the latest version of the underlying standards/specifications on which is has been built.		
3.	Application server must support integration with third party systems such as Databases, LDAP/AD, Messaging middleware, etc.		
4.	Integration with all Leading and Major LDAP and Active Directory tools and products.		
5.	Should have capability of Integration with DevOps tools for automated deployment of application releases.		
6.	Should support Industry standard web server		
7.	Solution must provide Out-of-the-box support for Horizontal and Vertical scalability, Clustering, Caching, Fail-Over & Load Balancing.		
8.	Solution must support HTTP session replication		
9.	Solution must support High-availability and JMS Clustering Support		
10.	Solution must support Data Source configuration and		

S. No.	Features	Availability (Y/N)	Remarks
	failover		
11.	Solution must support Dynamic Application Update with and without downtime (i.e., Cold and Hot deployments).		
12.	Should provide a secure, web-based administration and server management console that enables the authorized admin users to deploy applications/services and manage relevant configurations.		
Monitoring and Administration			
13.	It shall provide Diagnostic tools / log files that help to isolate the source of problems		
14.	Solution must support Deployment of multiple versions of the same application.		
15.	Enterprise level support Should be available 24X7 via E-Mail, helpdesk or contact centre such that unlimited production as well as development tickets may be raised for timely resolution.		
16.	Should have the ability to add or remove a node for maintenance from a web console without requiring any downtime.		
17.	Shall provide security infrastructure and mechanisms to protect sensitive application binaries, resources, security keys, digital signatures, and configurations from unauthorized access.		
18.	SSL must be supported		
19.	All modifications through the administrative infrastructure should be logged and be available for any audit.		
20.	Solution must support Thread pooling, connection pooling, customized pools		

18.5 Patch management

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed Patch management solution should have the capability to detect, collect and maintain information about patches currently deployed on the various components / services deployed on the Datacentres.		
2.	Patch management solution should be deployable on Cloud infrastructure.		
3.	Patch management solution should cater to applying of patches on Operating systems and other components / services proposed for CPP system.		
4.	Solution must support rapid trouble shooting and patch management reporting to verify if the servers have specific patches installed / updated		
5.	Solution must support code and application deployment on servers in single or multiple instances.		
6.	Solution must provide reports of patching activities in Cloud based Datacentres. This Includes out-of- the-box compliance reports and patch update statuses.		
7.	The patch deployment activities should be logged for reviews, analysis and audits.		
8.	The solution should have capability to export reports in multiple formats such as xls, pdf, csv, etc.		
9.	The system should enable cloud administrator to Patch any server/component/service from any Datacentre using a single console.		
10.	System should provide a shell interface to let users operate through a command line / command script across multiple servers simultaneously.		

18.6 Backup

For CPP Application, preventing the loss of data is paramount. Therefore, there is a requirement to have an additional back up of Application Data apart from the provisioned DC-2.

S. No.	Features	Availability (Y/N)	Remarks
1.	The additional Data backup should be taken on Cloud Platform.		
2.	Backup/archived data/files must be stored in a CSP Datacentre which lies at a distance of atleast 300 kms from either DC-1 or DC-2, even if it warrants engagement of a different CSP.		
3.	Solution shall provide de-duplicated backup and recovery services		
4.	Backup shall happen at designated schedule as per the policy defined by IA&AD		
5.	The solution shall have capability of logging and audit of backup activities. Logs shall be retained for at least 6 months		
6.	The solution must support backups including full, incremental and differential backups.		
7.	Backups should be monitored. Monitoring should have alert mechanism in case of a backup failure.		
8.	The solution shall have the capability to display backup activities through dashboard/reports		
9.	Required storage must be available in auto scale model in case backup sizes increase. It should not hamper ongoing backup process.		
10.	Backup should be available for all components, database, VM and configurations, so that entire solution can be recovered at a previous point in case of application issues.		
11.	Low-cost Storage should be utilized for storing the backup		

S. No.	Features	Availability (Y/N)	Remarks
	data.		
12.	The backups would consist of all the data including but not limited to files, folders, images, system state, databases and applications, etc.		
13.	Solution must provide encryption of all backup files and data.		
14.	Solution must provide capabilities to restore the backup / archived data.		

19 Security Services

The Bidder must ensure that each of the components listed in this section should be deployable on Cloud infrastructure.

19.1 Enterprise Security

The envisaged Enterprise Network Security for CPP System will include the following security components/services as single/multiple component(s).

1. Next Generation Firewall
2. Application Security with user authentication
3. VPN
4. IPS
5. URL filtering
6. Anti-APT Solution with sandboxing for Internet Zone
7. Threat Prevention

The features pertaining to each of the aforesaid items are listed below:

S. No.	Features	Availability (Y/N)	Remarks
Next Generation Firewall			

S. No.	Features	Availability (Y/N)	Remarks
1.	Next Generation Firewall should be deployable on Cloud infrastructure.		
2.	Firewall must consist of the following features: • SSL/TLS traffic inspection, Deep Packet Inspection (DPI) • Intrusion Prevention System (IPS) • Anti-Malware Application Security with user identification • URL filtering Note: Solution can be one integrated solution or combination of separate components.		
3.	CPP infrastructure and security architecture envisions the use of two firewalls as External (Perimeter) Firewall & Internal (MZ) firewall. These two Firewalls should be from different vendors.		
4.	Should have in-built capabilities for Inbuilt Anti-virus and Anti-Bot solution so that they are able to inspect HTTPS traffic on the fly for any infected file. These protections should work for protocols like HTTP, HTTPS, etc.		
5.	Seamless Integration with other security solutions such as Anti-APT, etc.		
Application Security with user identification			
6.	The proposed solution must allow policy rule creation for application control, user-based control, host profile, threat prevention, Anti- Malware / Zero-day, file filtering, & content filtering		
7.	The Solution must provide detailed analysis on sessions consumed, data transferred and threats involved as the CPP applications are used by their users.		

S. No.	Features	Availability (Y/N)	Remarks
Security and VPN			
8.	The Security platform should scan files transferred / Uploaded through CPP Applications for any Viruses / Malware content at runtime (during upload).		
9.	The proposed solution must support Policy Based control/forwarding based on: • Zone • Source or Destination Address • Source or destination port • Application (not port based) • AD/LDAP user or User Group • Services or ports		
10.	The security instance should support SSL VPN functionality		
Intrusion Prevention System			
11.	Intrusion prevention signatures should be built based on the vulnerability itself. A single signature should stop multiple exploit attempts on a known system or application vulnerability.		
12.	The proposed solution must support different Custom IPS and Application policies for different users and groups.		
13.	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, and reset both client and server.		
URL Filtering			
14.	The proposed device shall have custom URL-categorization and support customizable block pages		
15.	The proposed security instance shall have URL Filtering policies by AD/LDAP user, group, machines and IP		

S. No.	Features	Availability (Y/N)	Remarks
	address/range		
16.	Should have full-path categorization of URLs only to block the categories identified as the malicious malware path not the full domain or website		
17.	Should have zero-day malicious web site or URL blocking capability.		
18.	Should have URL or URL category base protection from phishing attack with malicious URL path		
Anti-APT			
19.	The proposed solution shall have sandbox behavior-based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP). The solution shall support automated signature generation for discovered zero-day malware.		
20.	The solution should be able to perform dynamic threat analysis on files such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, etc.		
21.	The proposed solution should be able to detect and prevent zero-day threats infection occurring through HTTP, HTTPS, FTP or by any of the application used by the users.		
Threat Prevention			
22.	The proposed security instance shall perform content-based signature matching beyond the traditional hash base signatures and should support SMB/NetBIOS traffic scan/inspection.		
23.	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules,		

S. No.	Features	Availability (Y/N)	Remarks
	protocol anomaly detection, and behavioral anomaly detection techniques.		
24.	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware.		
25.	OEM must provide evidence of the performance, throughput and features of their products/services through public domains- Websites and data sheets only.		

19.2 Web Application Firewall

S. No.	Features	Availability (Y/N)	Remarks
1.	The proposed WAF shall be dedicated or part of security solution with minimal latency		
2.	Should have high performance throughput to meet functional requirement of CPP		
3.	The component should be deployable on Cloud infrastructure.		
WAF should have the flexibility to be deployed in the following modes:			
4.	The solution must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.		
5.	WAF should support for IPv4 and IPv6 traffic		
6.	It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social AADHAR)		
7.	It should be able to extract the attack source IP address		
8.	Protection against Known & unknown types of Attacks and Security Threats.		
9.	The proposed WAF should support Security Filters such as,		

S. No.	Features	Availability (Y/N)	Remarks
	but not limited to, Brute Force Security Filter, Files Upload Security Filter, Web services Security Filter, Session Security Filter, etc.		
10.	The proposed WAF should support Activity Tracking & Reporting of Security incidents.		
11.	Solution should support automated Security Filter Policy Generation, Policy Updates and Deployment.		

19.3 Security Information and Event Management

S. No.	Features	Availability (Y/N)	Remarks
1.	The solution must provide central management and administrative functions of all systems/ components/services deployed by the Bidder/CSP from a single web-based user interface.		
2.	The administrator must be able to define role-based access to the systems by device, device group or area of network.		
3.	The solution must integrate with 3rd party directory systems (LDAP/AD) for authentication of the users accessing this solution.		
4.	The solution must support auto-discovery of assets/hosts on the network		
5.	The solution must provide a mechanism to track security events across a wide range of attributes (i.e. IP addresses, hostname, usernames, MAC address, log source, correlation rules, user defined, etc.) for all components/services deployed by the Bidder/CSP. The		

S. No.	Features	Availability (Y/N)	Remarks
	user must be able to filter events based on these defined attributes on the UI.		
6.	The solution must support an open standard API for integrating with other components such as Reporting solution, etc. to enable access to its information database(s).		
7.	The solution must support a web-based GUI for management, analysis and reporting.		
8.	The solution must ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., management console goes off-line all separate collectors still continue to capture logs).		
9.	The solution must have an automated backup/recovery process.		
10.	The solution must have the capability to automate its internal health checks and notify the user in case any problems arise.		
11.	The solution must provide the ability to deliver multiple dashboards/reports out of the box (such as for threat management, compliance management, etc.) that can be customized to meet the specific requirements of different users of the system as well as provide information of components/services deployed by the Bidder / SI.		
12.	The solution must provide the ability to visually represent event data. This will assist analysts in rapidly determining the impact of attacks and provide incident response and remediation.		
13.	The solution must maintain a database of all components/services discovered on the network (DC-1		

S. No.	Features	Availability (Y/N)	Remarks
	and DC-2). This data must include important information about the asset (such as user identity, system attributes, network attributes, vulnerability state, etc.).		
14.	The solution must provide facility to search for the statuses/logs/reports of a particular asset or asset group based on asset's attributes provided in search criteria.		
15.	The solution must integrate with other security and network solutions.		
16.	The solution must have the capability to scale up as the organization adds more components, services to the application.		
17.	The solution must support a database for event and network activity collection such that all information can be stored at a single source.		
18.	The solution must ensure the integrity of the information collected.		
19.	The solution must provide intuitive mechanisms for troubleshooting such as proactive notifications, command line utilities, console alerts etc.		
20.	The solution must support an out-of-the-box predefined correlation rules for identifying sequence of events which may be customized as per IA&AD requirements.		
21.	The solution must support user defined taxonomy and custom tagging of events and fields.		
22.	The solution must provide retrieval, aggregation, sorting, filtering and analysis of data across all distributed components.		
Log Management & Reporting Requirements			
23.	The solution must have a log collection and archive		

S. No.	Features	Availability (Y/N)	Remarks
	architecture that supports both short-term (online) and long-term (offline) event storage.		
24.	The solution should allow storage of logs/log archives/configuration files/backup on a storage platform that should not be a proprietary storage.		
25.	The solution must provide capabilities for efficient storage and compression of collected data.		
26.	The solution must support industry log collection methods (such as syslog, WMI, JDBC, Log File, SFTP, SNMP, Checkpoint LEA, etc.)		
27.	The solution must provide agent-less collection of event logs whenever possible.		
28.	The solution must support long-term access to detailed security event and network flow data. The system must be able to provide access to at least 12 months' worth of detailed information.		
29.	The solution should provide flexibility to add customized event fields in cases when SIEM is unable to categorize the events (eq. phone number, Aadhaar card number etc.).		
30.	The solution must support correlation of events from multiple vendor components/services and applications, enabling analysis and remediation of high priority threats.		
31.	The solution must provide the ability to store/retain both the log, packet and endpoint meta data and the original raw message of the event log for forensic purposes.		
32.	The solution must support log time stamps.		
33.	The solution must provide near-real-time and long-term trend & analysis of events.		
34.	The solution must provide more advanced event drill down		

S. No.	Features	Availability (Y/N)	Remarks
	when required		
35.	The solution must provide a real-time view that supports full filtering capabilities.		
36.	The solution must provide alerting based on observed anomalies and behavioural changes in network and security events.		
37.	The solution must support and maintain a history of user authentication activity on a per asset basis.		
38.	The solution must support the ability to schedule auto generation and auto distribution of reports.		
39.	The solution must provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues.		
40.	The solution must provide alerting based on observed security threats as well as anomalies & behavioural changes observed in monitored devices and network activity (flow) data.		
41.	The solution must provide the ability to correlate information across potentially disparate devices.		
42.	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)		
43.	The solution must support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc.		
44.	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
45.	The solution must provide UI based wizard and capabilities		

S. No.	Features	Availability (Y/N)	Remarks
	to minimize false positives and deliver accurate results.		
46.	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an E-Mail message.		
47.	The solution must integrate with security and threat intelligence data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating internal activity with external threats. These data feeds should be updated automatically by the solution.		
48.	The solution must monitor and alert when there is a disruption observed while generating logs from a component or service. E.g., if logs are not observed to be generated from a server in X minutes then generate an alert.		
49.	The solution must be able to pull in identity context from variety of sources in order to appropriately map user identity with current activity. Solution must be able to map multiple user aliases/attributes back to a single user.		
50.	The solution must provide the ability to send notification of correlated alerts via well-defined methods (i.e. SNMP trap, E-Mail, SMS, etc.)		
51.	The solution must provide embedded workflow capability that security operations staff can use to guide their work		
52.	The solution must provide integration with 3rd party trouble ticketing/help desk/ITSM systems through open-standard interfaces.		
53.	The solution must provide a mechanism to capture all		

S. No.	Features	Availability (Y/N)	Remarks
	relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.		
54.	The solution must provide a mechanism to annotate a security incident as it is addressed by the security operations staff.		
55.	DNS Malware Monitoring: The vendor's solution must provide capability to fetch events pertaining to malware-infected hosts and endpoints (i.e, VMs/Containers, components, services), and report these events on the UI.		
56.	The solution must provide capability to load balance incoming logs to multiple log collector instances.		

19.4 Data Loss Prevention

DLP is intended for deployment on Servers, VMs/Containers, etc. on CSP platform, as well as on the endpoints (Desktops, Laptops) of the Bidder's Development and O&M team resources working on CPP project. Bidder is free to choose a single solution or two different solutions for DLP deployed at CSP platform and team resources desktops/laptops.

S. No.	Features	Availability (Y/N)	Remarks
1.	DLP Solution should provide broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses.		
2.	DLP Solution should actively monitor the ways confidential data can be used on the endpoint and flags any activity not in accordance with policy defined from the centralized		

S. No.	Features	Availability (Y/N)	Remarks
	console.		
3.	DLP Solution should provide mechanisms to address and remediate intrusion attempts occurring on the endpoints.		
4.	DLP Solution should scan servers, laptop and desktop hard drives for confidential/Sensitive data in order to inventory, secure or relocate it and provide templates or equivalent to enable out-of-the-box discovery of sensitive data mapped to different industry and regulatory directives.		
5.	DLP Solution should scan for confidential/sensitive data when endpoint is idle and subsequent scans must run on only those things that have changed since the previous scan.		
6.	DLP Solution should provide following detection technologies to address different types of data, such as (but not limited to): a) Fingerprinting which looks for exact matches of whole or partial files, coming from structured sources (e.g., databases) and unstructured sources (e.g., design documents). b) Content which looks for data matching keywords, expressions or patterns, file type recognition, and other signature-based detection technologies.		
7.	DLP Solution should prevent confidential/sensitive files from downloading, copying to CD/DVD/ USB/iPod®/Bluetooth®, and other removable media; print screens, communications over E-Mail.		
8.	DLP Solution should monitor and prevent data using HTTP/HTTPS over browsers like Chrome, Firefox and Internet Explorer, etc. at endpoint.		

S. No.	Features	Availability (Y/N)	Remarks
9.	DLP Solution should monitor data being copied and pasted from the clipboard to prevent confidential/sensitive data from being pasted to specific application.		
10.	DLP Solution should provide trusted device support. This enables organizations to define specific removable media devices that can be used with confidential data, providing a more granular level of protection while still enabling required business functions.		
11.	DLP Solution should provide application file access control to prevent the use of confidential/sensitive data on social web sites on internet.		
12.	DLP Solution should automatically notify data owners of any policy violation.		
13.	DLP Solution should have a web-based management UI for defining, deploying, and enforcing data loss policies, responding to incidents, analyzing and reporting policy violations, and performing system administration.		
Data Loss Prevention (DLP) for E-Mail			
14.	DLP Solution should monitor mail communications and detects confidential/sensitive data that is being sent in violation of security policy. If a security policy is violated, it should block E-Mail communications.		
15.	DLP Solution must redirect, quarantine, or block outbound messages containing confidential/sensitive data. It must be deployed at egress points in the network DMZ and should integrate with your existing on-premise messaging infrastructure.		
16.	DLP Solution should quarantine or relocate E-Mail		

S. No.	Features	Availability (Y/N)	Remarks
	containing sensitive data to a secure location for end-user review and release.		
17.	DLP Solution should provide broad integration support for E-Mail services.		
18.	DLP for E-Mail should have integration with anti-spam solution.		

19.5 Host Intrusion Prevention System

HIPS will be deployed on all the servers at DC-1 and the DC-2.

S. No.	Features	Availability (Y/N)	Remarks
1.	The component should be deployable on Cloud infrastructure.		
2.	Solution should provide protection from all classes of attacks, including port scans, buffer overflows, Trojan horses, and worms.		
3.	Solution should provide Automated real-time intrusion detection. It should protect components/services by analysing the events, operating system logs and inbound/outbound network traffic on servers		
4.	The solution should allow creation of custom and location-based policies.		
5.	When an application attempts an operation, the HIPS should check the operation against the application's security policy, make a real-time allow or deny decision on its continuation.		
6.	HIPS must provide a Management Centre that provides all management functions for all HIPS agents in a centralized		

S. No.	Features	Availability (Y/N)	Remarks
	manner.		
7.	Solution must support Correlation of events to be performed on the Management Centre console.		
8.	Should protect the servers even when they are off network.		
9.	Should be compatible with the chosen operating system and server hardware.		
10.	HIPS should provide a web-based, user-friendly interface.		
11.	HIPS should provide out-of-the-box reports as well as capability to configure custom reports.		

19.6 Privilege Mgmt. of System Administrator

S. No.	Features	Availability (Y/N)	Remarks
Privileged Account Management System-Agentless			
1.	The component should be deployable on Cloud infrastructure.		
2.	The proposed solution must be at least accredited with Common Criteria EAL 4.		
3.	User's access to the proposed solution should be via encrypted channel only.		
4.	The solution should allow access of only authorized application/component/service functionalities based on the privileges provided to the logged in user. The system should be based on zero trust.		
5.	At the time of Login, the proposed solution should provide access to the users based on zero trust.		
6.	The proposed solution should allow to secure, manage, automate and log all activities associated with the		

S. No.	Features	Availability (Y/N)	Remarks
	privileged accounts for audit trail purpose.		
7.	The proposed solution should support password management as per CPP project's security policy and requirements.		
8.	Administrator should be able to create authorization policy for any User, Group (including dynamic groups), Role, or ad-hoc user(s).		
9.	The proposed solution should share a common infrastructure for managing, securing and tracking shared privileged accounts.		
10.	The proposed solution should be browser independent and there should not be any browser dependency to manage and record the sessions.		
11.	The proposed solution should enforce users to specify reason when requesting access for a privileged account.		
12.	The proposed solution should have the facility to generate new password automatically every time the user tries to login.		
13.	The proposed solution should be policy based and should be used to configure different policies for privileged accounts on different platforms and components.		
14.	The proposed solution should have alert system to notify the Approver when a new request has been put up for his approval.		
15.	The proposed solution should support strong authentication through mechanisms such as 2-factor, Radius, RSA, LDAP and RSA + LDAP, etc.		
16.	The proposed solution should support communications with LDAP compliant directory servers to obtain user		

S. No.	Features	Availability (Y/N)	Remarks
	identification, user role and security information.		
17.	The proposed solution should provide web browser-based UI for users to perform activities such as account management, privilege request, approval, viewing audit trail, etc..		
18.	The proposed solution should support dual approvers control as part of the workflow for privileged account password request, if required.		
19.	The proposed solution should have the capability to enforce time-limited secure remote access of CPP environments without having to expose credentials to external users e.g., providing guest login to 3rd party vendor staff, etc.		
20.	The proposed solution should enable archival of audit logs.		
21.	The proposed solution should generate audit trail reports for reviews and analysis.		
22.	The proposed solution should have session timeout capabilities, when session remains idle and this parameter should be configurable.		
23.	The proposed solution should have capability of integration with SIEM for log forwarding.		
24.	The Proposed solution should have ability to manage local administrator credentials of components/services of CPP system.		
25.	The Proposed solution should have High Availability and should have ability to provide real-time data synchronization with its other instances deployed in a cluster.		
26.	The proposed solution should create isolation between the		

S. No.	Features	Availability (Y/N)	Remarks
	privileged user's desktop and the target system, which eliminates the risk of planting malware on critical systems.		
27.	The proposed solution should control, monitor and record all privileged sessions.		
28.	The proposed solution should be able to map local drive or directory during an RDP session.		
29.	The proposed solution should be able to auto discover devices in the network segment range.		
30.	The proposed solution should provide full session recording.		
31.	The solution should have the ability to perform SHA verification every time the session recording is being played or provide tamper proof session recordings features to ensure the session recording integrity is not compromised.		
32.	The proposed solution should provide facility with proper access control mechanism for the retrieval and viewing of the recorded privileged sessions.		
33.	The proposed solution should compress the session recordings to reduce the need for excessive storage.		
34.	The proposed solution should support privacy regulation by allowing on-screen user notification when a session is being recorded.		
35.	The proposed solution should be able to prevent leap-frog attempts.		
36.	The proposed solution should support the use of native SSH client, e.g. Putty, by creating a SSH tunnel through the proposed solution and still able to blacklist or whitelist command, SSO, and record session.		
37.	The proposed solution should allow for backup of the		

S. No.	Features	Availability (Y/N)	Remarks
	policies that is set in the proposed system which can also be easily imported to another proposed system.		

19.7 Database activity monitoring

S. No.	Features	Availability (Y/N)	Remarks
1.	The Database activity monitoring solution should be compatible with the Database proposed by the Bidder for the CPP Application.		
2.	The solution should be capable of monitoring all activities pertaining to all databases proposed by the Bidder for the CPP system. Activities should also be monitored for all types of users accessing the database either through applications or directly at the host, including login/logout. Monitoring must be done for all DDL/DCL/DML commands/Queries/Transactions, all administrator commands such as Grant, Revoke etc., executed on the Database. Detailed information should be captured in real-time and reported at granular level with all relevant details such as executed by, Query title, Date & time of execution, Input parameters used, Source IP, Database instance/schema, tables accessed, values affected, etc.		
3.	Solution must have the capability and configurability of sending alert notifications for specific Database activities.		
4.	The administration of the solution should support segregation of duties based on roles/groups etc.		
5.	The solution should be able to integrate with LDAP		
6.	The solution should be deployable on Cloud in virtual		

S. No.	Features	Availability (Y/N)	Remarks
	environments		
7.	The solution should have capability to facilitate allowing/blocking users from accessing Database/DB objects based on user roles and security policies.		
8.	The solution can be configured to support both detection and prevention of unauthorized activities.		
9.	The solution should be capable to kill user sessions for cases such as accessing sensitive data, instances of policy violations, etc., and keep all activity in the logs.		
10.	The solution should be able to monitor and block security attacks like SQL Injection, Denial of Service in real time and generate alerts.		
11.	The solution should be able to send detailed logs to SIEM.		
12.	The solution should have reporting/ integration capabilities through syslog/SNMP		
13.	Solution should provide centralized, tamper-proof audit repository for audit data collected from multiple database types. The log files should be stored within the solution for atleast 6 months.		
14.	Should be able to collect, aggregate and normalize activity logs from database.		
15.	Should be able to share automated reports through E-Mail.		
16.	Should be able to control access to database on the basis of source IP(s).		
17.	Should be able to recognize a higher volume than normal transactional volume from a particular user and generate alerts		
18.	The solution should be able to auto-discover all databases objects for the CPP project, including any new database that		

S. No.	Features	Availability (Y/N)	Remarks
	is created during the life of the project.		
19.	The solution should be able to auto discover privilege users in the database.		
20.	The solution should be able to auto discover default passwords in the default DB accounts.		
21.	The solution should be capable of monitoring operations being done on the sensitive/confidential database objects, like Aadhaar numbers, as per defined rules, and report operations performed on this data.		
22.	The solution should provide easy pre-defined policy/rule creation templates for monitoring of Database objects and queries.		
23.	Automated mechanism for updating security configurations/policies across multiple databases.		
24.	Can track and alert all failed logins.		
25.	Can track the dormant accounts as per defined rule.		
26.	The solution should be able to schedule and distribute the reports automatically as per configurations.		
27.	Solution should be capable of tracking, identifying and logging activities performed by DBA (without network access, using OS authentication) through the console.		
28.	The solution should support creation of user defined reports without using any third-party solution. Reports should have filtering and sorting capabilities.		
29.	The solution should be capable to have an executive dashboard to provide a summary view based on user defined criteria, with support to drill down the presented data.		
30.	The solution should be able to generate the reports in		

S. No.	Features	Availability (Y/N)	Remarks
	HTML, PDF, Excel formats as per requirement of the user.		
31.	The solution should discover misconfigurations in the database and suggest remedial measures.		

19.8 Hardware Security Module

HSM shall be used or storing digital keys and certificates that will be required by the application for encrypting sensitive data such as Aadhar numbers, PII data, documents, etc.

S. No.	Features	Availability (Y/N)	Remarks
1.	Should support all OS proposed by the Bidder for CPP System.		
2.	HSM solution must be deployable on Cloud infrastructure.		
3.	HSM must be FIPS 140-2 Level 3 compliant.		
4.	Solution should support fine-grained policy to enable administrator to ensure that the Encryption keys and Digital Signatures are secured against any unauthorized access.		
5.	Solution must have the capability to store Class III digital certificates.		
6.	Proposed solution should support multi-tenancy with each tenant having its respective configurable policies, key management and audit log.		
7.	Should have comprehensive logging and reporting functionality		
8.	Should support access of logs to SIEM for activity monitoring.		
9.	Should support Network Management capabilities such as SNMP, NTP, Syslog over TCP		
10.	HSM must support non-disruptive key rotation. Key		

S. No.	Features	Availability (Y/N)	Remarks
	rotation must be supported on live transformation of data with no downtime.		
11.	Administrator of Key Manager should authenticate using 2FA solution		
12.	Should integrate with users and groups from LDAP, local systems, container environments etc.		
13.	The package must include a single management (Device Manager) application to install and configure HSM.		
14.	The HSM must comply with current GoI, CCA guidelines for storing and managing the Digital keys/certificates.		

19.9 Anti-Virus malware and Anti-Spam

Anti-virus, malware and Anti-Spam shall be used at the Servers deployed in the Cloud Datacentres by the Bidder. These need not be provisioned for the endpoints (Desktops/Laptops) of the Development and O&M teams of the Bidder and the IA&AD teams who will be working on CPP project.

S. No.	Features	Availability (Y/N)	Remarks
1.	Solution should be deployable in Cloud infrastructure.		
2.	Should support deployment on all OS proposed by the Bidder for CPP System.		
3.	Solution should analyse incoming data and block threats while they travel through the network before hitting the system. Rules-based browser protection should be included to protect against web-based attacks.		
4.	Solution should have signature-based antivirus, which should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.		

S. No.	Features	Availability (Y/N)	Remarks
5.	Solution should correlate linkages between users, files, and websites to detect threats by analyzing key file attributes. Solution should accurately identify if file is infected and effectively protect against targeted attacks.		
6.	Solution should allow only whitelisted applications to be accessed on the System.		
7.	Solution should identify and protect security breaches by monitoring application behaviour and controlling file access, registry access, permitted processes.		
8.	Administrator should be able to verify and report compliance. Solution should isolate a non-compliant or infected system and quarantine infected file.		
9.	Should automatically detect what location a system is connecting from, such as intranet and internet and adjusts the security to offer the best protection for the environment.		
10.	Solution should automatically switch to aggressive scan mode if the AV client detects a large number of viruses, spyware, or high-risk threats to clean/delete/quarantine these threats.		
11.	Solution should provide graphical display to manage and monitor content distribution providers or group update providers in our environment. It should also provide health and content distribution status of group update providers.		
12.	Solution should provide out-of-the-box set of reports for management and administrators.		
13.	Solution must provide necessary capabilities/ interfaces to enable detection of any virus/malware content at runtime		

S. No.	Features	Availability (Y/N)	Remarks
	while uploading any file from the CPP applications. The anti-virus/anti-malware checks should not disrupt the application workflow and must provide a seamless end user experience. It must give an error message back to the web/service/request in case the file is found to be infected with malware.		

19.10 Identity & Access Management (IDAM)

Please refer Vol-1 Annexure B Section 6.2.3 for requirements pertaining to Access control of Business users. An IDAM solution for back-office users should have the features listed in following table.

S. No.	Features	Availability (Y/N)	Remarks
1.	Solution should be deployable in Cloud infrastructure.		
2.	Solution must have the capability to integrate with LDAP system and provide Open-API for integration with other CPP applications/components/services.		
3.	Support Creation and management of Identity of Users, Groups and other objects present in CPP System along with their respective attributes and associated identifiers.		
4.	Should support automated account creation, modification, suspension, and deletion across systems and applications based on changes in the Roles and Entitlements of a user.		
5.	Solution should provide the capability to manage profiles and privileges of all Business Users and Groups across all application services and components through a single management interface.		
6.	Solution should have the capability to enforce privileges and access policies for a business user group across all CPP		

S. No.	Features	Availability (Y/N)	Remarks
	application components and services. Addition or removal of a business user from a specific User group should automatically translate to appropriate modifications in privileges assigned to that user across CPP components and services.		
7.	Solution must provide capability to authenticate the user at the time of login and provide access to only those applications/resources/services that the user is authorized to after successful authentication.		
8.	Should support synchronization of identity information to various repositories/ directories. Synchronization can be event based or time based.		
9.	Should support Identity merging and splitting		
10.	Should support delegated Identity administration		
11.	Should support configurable password policies (including format, expiry, etc.) as per CPP project's requirements.		
12.	Should support configurable OTP policies (including OTP format, timeout, etc.) as per CPP project's requirements.		
13.	Should be capable of generate robust, random passwords (as per CPP project's requirements) in case of new account creation and password reset etc. and send it through E-Mail and SMS (through multiple service providers).		
14.	Should support sending OTP on E-Mail and SMS (through multiple service providers) simultaneously.		
15.	Should be able to create a Group of synthetic users which will be allowed to access the application without 2FA.		
16.	Should support self-service password resets		
17.	Should support account reconciliation		
18.	The solution should support time or location-based policies.		

S. No.	Features	Availability (Y/N)	Remarks
19.	Solution should support automatic failover to other IDAM instance in case of disaster at primary instance.		
20.	Should support platform/component/service specific provisioning and de-provisioning connectors		
21.	Solution must provide API/services that support workflow capabilities.		
22.	Should support access request management. Ability to provide a consistent and auditable process for requesting and approving access privileges.		
23.	Should have robust reporting capability to include ad hoc reporting.		
24.	Must support Single-Sign on technology to manage all credentials of a given user across many technology platforms including web and non-web-based applications		
25.	Solution must ensure that the identity information and all user credentials are encrypted in storage as well as in transit between all components of the system.		
26.	The solution should support context specific step-up from password authentication to 2-factor token authentication when more sensitive data or functions are requested by a user. Administrator should be able to control the priority / method of authentication through configurations.		
27.	Should support authentication and authorization for users accessing the applications from other devices such as PDAs, Mobile phones etc.		

19.11 Single Sign-on (SSO) and Single Logout

S. No.	Features	Availability (Y/N)	Remarks
1.	The Product must support Open Standards like SAML 2, oAuth 2, OpenID Connect, WS-Security and WS Federation		
2.	Should integrate with existing LDAP / IDAM solution		
3.	The Product must support Implementation of SAML 2 Identity Provider and SAML 2 Service Provider for authentications based on SAML2		
4.	The product should support secured communication between different components using SSL		
5.	The Solution should support session timeout for idle sessions and single log-out.		
6.	Should support access of logs to SIEM and other security components for activity monitoring.		
7.	SSO must support reverse proxy for all application components.		
8.	The application must be an integrated solution. All the components of the application should support single sign-on and single logout. Application components may include BPM, BRM, DMS and KMS related functionalities, etc. The application experience for the end-user with respect to login, session management and logout should be seamless and synchronous. Bidder should evaluate the need of having an appropriate solution that allows only necessary access to the users based on their profile/role.		
9.	The session timeout for different components of CPP application would be synchronous and will be decided by IA&AD.		

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

**********The End**********