Annexure 16 - Technical Requirements

Instructions for Filling up Annexure

Column A **"Sr. No." - Serial Number of the requirement provided by UIIC. The bidder must not change any information in this column**

Column C **"Technical Requirements" - The detailed Requirement. The vendor must not change any information in this column**

Column D **"BR" - Bidder Response – The bidder would be required to provide an appropriate score to each requirement requested for as per the following tab**

Sno.	Description
a	Yes - Bidder will deliver the given requirement and has included the efforts in the estimates.
b	No - Bidder will NOT deliver the given requirement and has NOT included the efforts in the estimates.

NOTE: If the scoring was not mentioned in any of the row item by bidder in annexure, then that parameter will be considered as 0

Column E **"Bidder Comments" - The Bidder is free to provide any Comments the bidder wishes.**

Authorised Signatory

Name and Designation Official Seal

Date:

Place:

This annexure covers the Technical Requirements expected from the solution and all the associated technology components and the Non-Functional Specifications expected to be delivered by the bidder through this solution as per the scope outlined in the RFP

A. Technical Requirements			Bidder Response	Remarks
S. No	Area	Requirements		
Architecture				
Tech-0001	General - Architecture	The Bidder should describe the overall Functionality/Business Architecture of Solution.		
Tech-0002	General - Architecture	The Bidder should describe the overall Logical Components in application architecture.		
Tech-0003	General - Architecture	Architecture should cover areas such as: Technology/System architecture, platform technology and development framework for customizing applications and interfaces, protocol for integration between Solution and other system.		
Tech-0004	General - Architecture	The Bidder should explain the configuration / parameterization capabilities of the system. The Bidder should explain ease of doing configurations/parameterization within the system directly to UIIC users to reduce the dependency on the Bidder to perform such activities.		
Tech-0005	General - Architecture	Platform should provide web-based n-tier architecture		
Tech-0006	General - Architecture	Platform should manage appropriate Tenancy ensuring application and data security with adherence to UIIC's policies/Statutory/Regulatory guidelines		
Tech-0007	General - Architecture	Should support multi- tier microservice oriented architecture (The Application should at least have the following within it's architecture) for all modules within the application with well defined interfaces between the layers: - Presentation Tier - Business Logic Tier / Transaction tier / Service Tier(Web Services Out of Box) - Data Tier (if Object Relational Model layer is used - please specify details)		
Tech-0008	General - Architecture	Platform/Solution should be cloud ready and Cloud agnostic with capability to be either deployed on any standard cloud, on-premise or as a hybrid solution with capability to be implemented as a containerized deployment . Please elaborate on deployment options.		
Tech-0009	General - Architecture	Application should have a loosely coupled modular structure providing the flexibility to deploy selected modules-products- lines of business combination as per the UIIC's decisions and preferences		
Tech-0010	General - Architecture	It should support the deployment of additional modules at a later point in time with minimal downtime and loss of productivity.		
Tech-0011	General - Architecture	System should support policy issuance and related transactions such as Claims, Endorsements etc via a User interface, Batch upload (XML, .csv), real time API services and Messaging based interfaces. The application should support MQ and JMS protocols for message queues.		
Tech-0012	General - Architecture	Application should be loosely coupled through service interfaces built on SOA based architecture. Below mentioned points are SOA related points and the vendor has to comply to the same. Please specify any standard reference architecture of used in the product.		
Tech-0013	General - Architecture	Application layer should hide all business logic from the frontend or the interface (Presentation layer) using well defined interfaces		
Tech-0014	General - Architecture	Application layer should hide all data access logic from the business logic through well defined interfaces		
Tech-0015	General - Architecture	Application should support integration of new services seamlessly into existing structure without significant changes or effort. If there is coding effort required please mention explicitly.		
Tech-0016	General - Architecture	Application should support option of rollback of transactions when the process is terminated in the middle including options like Rollback completely / Rollback to the nearest safe point / No rollback at all specifically in multi process operations		
Tech-0017	General - Architecture	The system should be enabled for crosscutting, non-functional capabilities in the platform thus relieving individual applications of this burden to reduce duplication. Capabilities should include Authentication (application to application Authentication), Security, Logging, Monitoring, Error handling and Recovery, Auditing, Deployment, and Dashboard.		
Tech-0018	Architecture Principles	The platform should be built on modern application (Microservice based) architecture using API first approach		
Tech-0019	Architecture Principles	Platform should support event driven design		
Tech-0020	Architecture Principles	Platform application should be containerized and orchestrated		
Tech-0021	Architecture Principles	Platform architecture should support zero trust design principles		
Tech-0022	General - Architecture	Ability to support Low Code /No Code methodology for design of workflow/reports as per the requirements / applicability to any technology component		
Tech-0023	General - Architecture	The Application should be SOA compliant		
Tech-0024	General - Architecture	Capability to support data quality checks/validations (configurable) and controls at data entry.		
Tech-0025	General - Architecture	System must maintain data Quality and integrity particularly at data capture, data flight and data at rest		
Tech-0026	General - Architecture	The Solution should be secured and scalable for enhanced add-on services as per industry standard.		
Tech-0027	General - Architecture	Capable to be interfaced with solutions using standard secure integration but not limited to API/SFTP/Message Queues/Database's interface through DB driver/Staging table etc.		
Tech-0028	General - Architecture	Solution should have staging area to hold the data & documents to facilitate the completion of transactions and user journeys on the platform. Post the journey completion, the data & documents to be synchronized with Core system / Datawarehouse / DMS. This is required for all the user journeys on all applicable portals		
Tech-0029	General - Architecture	Solution should store the metadata information for the documents that are stored in DMS to retrieve relevant documents from DMS when required.		
Tech-0030	Application Architecture	Ability to extract data from source documents but not limited to pdf, CSV, excel and email.		
Tech-0031	Application Architecture	The platform should have in-built feature to integrate with existing LDAP, OAuth, Active Directory or any third party identity management system		
Tech-0032	Application Architecture	Interaction between logic component, application packages, databases, and middleware systems in terms of functional coverage.		
Tech-0033	Application Architecture	Should have a robust Development Framework for application customization		
Tech-0034	Application Architecture	UI Designer to create page, layout, form, fragment, widget and also default template		
Tech-0035	Application Architecture	The Bidder should provide details about supported and un-supported browsers		
Tech-0036	Application Architecture	The solution should be capable of intelligent placement for workloads, so that the load gets distributed dynamically without any manual intervention and get efficient performance. This should be integral part of the solution and should not insist on any specific hardware make or model		
Tech-0037	Native Mobile Apps	Customer Portal and Distributor portal should also have a Native Mobile Application supporting all the functionalities of the portals.		
Tech-0038	PWA (Progressive Web App)	All the portal should be developed with PWA methodology to allow users to access the portals from multiple device types (Browser, Mobile App, tablet etc.)		
Tech-0039	PWA (Progressive Web App)	The solution must support responsive design for web and adaptive UI for mobile, while maintaining a shared component library wherever possible.		
Tech-0040	PWA (Progressive Web App)	Develop PWA in a manner to enable offline access for critical features and cached content (to the extent possible and in line with business requirements)		
Tech-0041	PWA (Progressive Web App)	Implement background sync for queued actions (e.g., form submissions) when offline, syncing automatically when connectivity is restored.		
Tech-0042	PWA (Progressive Web App)	The PWA should support Add to Home Screen functionality and provide an app-like experience without requiring app store installation.		
Tech-0043	PWA (Progressive Web App)	Enable web push notifications for user engagement, with proper opt-in and DPDP compliance.		
Tech-0044	PWA (Progressive Web App)	The solution must achieve optimal PWA performance ensuring fast load times, optimized caching, and minimal network dependency.		
Tech-0045	PWA (Progressive Web App)	All PWA interactions must occur over HTTPS, with proper security headers and protection against common vulnerabilities		
Tech-0046	PWA (Progressive Web App)	Business logic, API integrations, and state management should be shared across web and mobile.		
Tech-0047	PWA (Progressive Web App)	Solution must use a cross-platform framework that supports building web (with PWA capabilities) and native mobile apps from a single code base.		
Tech-0048	PWA (Progressive Web App)	The architecture should allow common business logic, API integrations, and state management to be reused across web and mobile platforms, minimizing duplication.		
Tech-0049	Omni-Channel Experience	Solution should follow "Omni-channel" principle while designing the functional and technical specifications for the components. This includes the entire Insurance Value Chain covering New Business, Issuance, Servicing, Claims, Employee portals etc.		
Tech-0050	Omni-Channel Experience	Platform should provide UI layout with omnichannel experience, by unifying all communication channels to achieve fail-proof uninterrupted customer communication while maintaining same customer experience ,productivity and quality of all interactions		
Tech-0051	Prudence in Journey Design	The Bidder must be design journeys/solution ensuring that unnecessary service calls (external services which have per transaction cost) are minimized or optimally used to reduce costs effectively while maintaining the required functionalities		
Tech-0052	Back End	Needs to adopt following from ground up design a. Encapsulation b. Re-usability c. Extensibility d. Scalability e. Maintainability		
Tech-0053	Back End	Needs to adhere to following standard design principles a. SOLID b. KISS (Keep It Simple) c. Modularity d. Coupling and cohesion of modules e. LEAST f. Cross cutting concerns g. DRY (Don't Repeat Yourself)		
Tech-0054	Back End	Needs to have clear decoupling of front end and back end (Separation of concerns) applications		

Tech-0055	Back End	Main architecture components are centralized e.g. a. API management b. Enterprise service bus (ESB) c. Document management system (DMS) d. Business rules engine (BRE)		
Tech-0056	Back End	Backend processing systems/modules (including Middle Office modules) needs to be designed with business perspective in alignment with business requirements		
User Access Management				
Tech-0057	User Access Management	There should be comprehensive User management system. It should be able to create different levels of users with different access to features. There should be templates for a group of users such as Administrators, Employees, branch office and so on. System should facilitate the creation of different levels of users and assigning different levels rights. There should be provision for disabling a user temporarily or on permanent basis.		
Tech-0058	User Access Management	Platform should provide centralized, policy-based authentication and single sign-on from any device including desktops, laptops, and mobile devices		
Tech-0059	User Access Management	Platform should have capability of onboarding new users (customers , Agents, Distributors and other required users), creating id and providing appropriate authorization for them		
Tech-0060	User Access Management	Platform should have the capability to integrated with any existing UIIC system to either generate or fetch user ids if in case users are created outside of the platform		
Tech-0061	User Access Management	Platform should have capability of onboarding new customers, creating id / golden id (in case of multiple policies) and providing appropriate authorization for them		
Tech-0062	User Access Management	Platform provides standards-based secure propagation of identity across applications and APIs		
Tech-0063	User Access Management	Ability to define access to specific menus by user groups. Specify levels of granularity and configurability		
Tech-0064	ID & Password Management	Define User ID and Password policy guidelines:		
Tech-0065	ID & Password Management	Enforce the use of individual ids and passwords to ensure accountability		
Tech-0066	ID & Password Management	Allow users to select and change their own passwords		
Tech-0067	ID & Password Management	Enforce password composition rules		
Tech-0068	ID & Password Management	Enforce password lockout of not greater than five (5) attempts		
Tech-0069	ID & Password Management	Force users to change temporary passwords at first login or use an approved one-time password		
Tech-0070	ID & Password Management	Maintain a record of previous user passwords to prevent re-use of the prior 05 passwords (configurable)		
Tech-0071	ID & Password Management	Not provide specific feedback to the user if a portion of or all of the login information is entered incorrectly		
Tech-0072	ID & Password Management	Only indicate login failure after both the identifier and authentication information have been entered		
Tech-0073	ID & Password Management	Display (upon successful logon) the number of unsuccessful login attempts made since the last time the user successfully logged in and display the date and time of last prior successful login		
Tech-0074	ID & Password Management	Not display or allow printing of passwords on the screen while being entered		
Tech-0075	ID & Password Management	Passwords must be stored in an encrypted format		
Tech-0076	ID & Password Management	Not provide help messages during the login process that would aid an unauthorized user		
Tech-0077	ID & Password Management	Force changes of passwords after X days (X to be configurable)		
Tech-0078	ID & Password Management	Allow for end users to change their password no more often than once per day and ask OLD password on change		
Tech-0079	ID & Password Management	Passwords must be alphanumeric containing at least one non-alphabetic character such as a numeral (0-9) or special character, where technically possible.		
Tech-0080	ID & Password Management	Passwords must not be prefixed or suffixed with a number, where technically possible.		
Tech-0081	ID & Password Management	System must not be configured to have a blank or null password. Blank or null passwords are not allowed for authentication.		
Tech-0082	ID & Password Management	Allow customized ID-password policies to be implemented.		
Tech-0083	ID & Password Management	Secure Password Policy implemented and validated on server side. (Minimum Password length, Password Complexity, Password history etc.)		
Tech-0084	ID & Password Management	Provision for password expiry and management. The system should have a question / answer along with the password reset before activating the reset password.		
Tech-0085	ID & Password Management	Password reset Link should expire after use/ after certain time period/ after fresh reset link sent		
Tech-0086	ID & Password Management	Password auto complete should not be enabled		
Tech-0087	ID & Password Management	Default password should not be allowed for use (on Login, forget password, change password pages)		
Tech-0088	ID & Password Management	System should not allow to change passwords for any other user. User should be able to use password rest function		
Tech-0089	ID & Password Management	Password should not be shown in clear text		
Tech-0090	User Access Management	Provide easy access to define new user groups and create custom roles. Administrative module / utility that allows a helpdesk to manage user / role creation.		
Tech-0091	User Access Management	Maintain administrative IDs for the purpose of system administration. The ability to extract all the user ID and details at any point of time.		
Tech-0092	User Access Management	The system should be capable of displaying a banner stating company policy for usage after login. This will apply to both the Core System		
Tech-0093	User Access Management	Password policy should be enforced on the portal (Admin account), application (User account) and servers including: - Password history - Maximum age - Complexity and Length of the password - Invalid login attempts permitted - Account lockout duration - Password reset mechanism - The system should have a question / answer along with the password reset before activating the reset password - The system should force change of password on first time login, first time login post reset		
Tech-0094	User Access Management	Platform should allow different categories of user login using different methods including Multi-factor Authentication		
Tech-0095	User Access Management	The system shall support secure login ID and passwords for each user and passwords shall be stored in encrypted format in database using strong crypto algorithm which are not deprecated/ demonstrated to be insecure/ vulnerable.		
Tech-0096	User Access Management	Ability of the application to integrate RBAC (Role Based Access Control) matrix as per UIIC requirements		
Tech-0097	User Access Management	Capability to provide different functionality to user according to their role.		
Tech-0098	User Access Management	Ability to control access rights at field level.		
Tech-0099	User Access Management	Users management (on Server for centralized application) should be available to Administrator(s).		
Tech-0100	User Access Management	The system shall provide support for Active Directory & LDAP support for integrating with directory services		
Platform Administration And Security				
Tech-0101	Platform Administration And Security	Platform should have admin module with capabilities to a. Register users and create user id / golden id (in case of multiple policies) b. Set up user roles and authorization and assign them to users appropriately c. Onboard and set up distributors across insurance companies and distribution networks d. Product set up and configuration e. Overall platform support and maintenance		
Tech-0102	Platform Administration And Security	Platform should provide 256 bit AES based encryption for data in rest and TLS 1.3 based encryption for data in transit allowing an end-to-end secure connection		
Tech-0103	Platform Administration And Security	Platform should be able to delegate some additional functionality at the user level, e.g.: change password functionality should be given to user.		
Tech-0104	Platform Administration And Security	Platform should be configured such that the relevant screens and system function shall be available to Agents, customers etc, but with role based access in place (i.e. a person can only access modules for which they have permission).		
Tech-0105	Platform Administration And Security	Single sign on, password encryption should be provided by the platform. Passwords should be configurable and stored in application database in encrypted format		
Tech-0106	Platform Administration And Security	Audit Trail and Maintain Log to be maintained for all transactions/ changes		
Tech-0107	Platform Administration And Security	Restricted read/write(create/update) access to menus based on user profiles. Should facilitate defining security (read, write, delete, edit) at multiple levels e.g. User, Role / Group, Menu, Menu Item, Form/Page, Field, etc.		
Tech-0108	Platform Administration And Security	Error Log and Unique error codes to be maintained on the platform		
Tech-0109	Platform Administration And Security	Complete and comprehensive security from unauthorized access and misuse should be available along with necessary audit trail detailing every user's activity on the platform		
Tech-0110	Platform Administration And Security	For platform Maker/ Checker feature should be enabled and several levels of users should be maintained		
Tech-0111	Platform Administration And Security	User names and passwords must be hashed or encrypted at storage as well as before passing them over the network for authentication purpose. Hashing should confirm to at least SHA2+Salt as well as strong crypto algorithm must be used which are not deprecated/ demonstrated to be insecure/ vulnerable.		
Tech-0112	Platform Administration And Security	Should support at least 256 bit encryption between web browser & web server front end (Internet & Intranet)		
Tech-0113	Platform Administration And Security	System should be implemented in secured coding practices, OWASP etc. to ensure 100% security of the Solution		
Tech-0114	Platform Administration And Security	System should have ability to dynamically control and manage information security by allowing content owners to decide who gets to view, edit, print or forward emails and documents and who does not.		
Tech-0115	Platform Administration And Security	Proposed system should be able to disable the copy/paste and screen capture capabilities		
Tech-0116	Platform Administration And Security	Proposed system should expire or revoke document access at any time		
Tech-0117	Platform Administration And Security	Should support strong authentication technology (Multi-factor) (Internet & Intranet)		

Tech-0118	Platform Administration And Security	Product should support web services standards namely WS* specifications from OASIS and W3C		
Tech-0119	Platform Administration And Security	Application should provide role based authorization which should be enforced through proper session management or privilege check for every action		
Tech-0120	Platform Administration And Security	The proposed solution should be able to log; All actions taken by any individual with root or administrative privileges. Access to all audit trails. All elevation of privileges. All changes, additions, or deletions to any account with root or administrative privileges.		
Tech-0121	Platform Administration And Security	Service provider shall conduct security testing for applications, all plugins and web services planned/ exposed for Web Server		
Tech-0122	Platform Administration And Security	Audit and Compliance Management: Platform to enable suitable information security / cyber security and secure configuration in respect of the components, and utilities in the system, as per requirement of UIIC from time to time. Continuous risk assessment and control process of the Bot to be conducted and probability of each risk along with impact to be evaluated and to be provided proactively periodically to UIIC team.		
Tech-0123	Platform Administration And Security	Security & Confidentiality: Platform should provide security capabilities such as encryption (e.g. AES256), data privacy, multi-factor authentication and Role Based Access Control policies to effectively leverage enterprise data sources.		
Tech-0124	Platform Administration And Security	Bidder should comply with all the guidelines issued by DFS/RBI/IBA/Govt. of India, IT ACT, Statutory requirements and any other regulatory authority from time to time at no additional cost to UIIC and should adhere to the security policies set up by the UIIC.		
Tech-0125	Platform Administration And Security	Service provider shall ensure that user access gets revoked on the last working day		
Tech-0126	Platform Administration And Security	Service provider shall provide details of Freeware / Open Source software used		
Tech-0127	Platform Administration And Security	The application should be configured such that the access to the customer information must support user level authentication and access rights		
Tech-0128	Platform Administration And Security	The application should be configured to enforce role-based access based on users, groups, roles, etc.		
Tech-0129	Platform Administration And Security	The application should be configured in such that the same screens and function shall be available to users but with role based access in place (i.e. a person can only access modules for which they have permission).		
Tech-0130	Platform Administration And Security	The application should be implemented to delegate some additional functionality at the user level, e.g.: change password functionality should be given to user.		
Tech-0131	Platform Administration And Security	The application should be configured to be deployed as a secured, managed desktop, allowing users ,access to only the programs they are allowed to use.		
Tech-0132	Platform Administration And Security	The system must NOT allow for any copies to be made of the document for modification purposes when the records are requested for access		
Tech-0133	Platform Administration And Security	Must allow tighter security of files while improving collaboration by making data sharing easy		
Audit Trail and Logging				
Tech-0134	Audit Trail and Logging	The solution should be configured to provide audit trail facility to track the users activities on all cases/workitems		
Tech-0135	Audit Trail and Logging	The solution should be configured to "pick up where left" in case of drop off customers. It should also keep a track of the customer's activity and show a history of activity done on the account.		
Tech-0136	Audit Trail and Logging	The application should be configured to gather and analyse data related to handling of customer issues, to help determine future customer care strategies		
Tech-0137	Audit Trail and Logging	The proposed solution should provide capabilities to monitor critical application service availability and should integrated with UIIC's application for providing alert for the servers.		
Tech-0138	Audit Trail and Logging	The company or other regulatory bodies like CERT-IN that govern the company reserves the right to audit (surprise as well as planned) operational processes and information security controls implemented at the Service provider to ensure compliance with Service Providers information security policy and controls and other controls as mandated as a part of this agreement		
Tech-0139	Audit Trail and Logging	Service provider shall have a defined process towards managing and monitoring of logs including its retention for DB, Server & Application		
Tech-0140	Audit Trail and Logging	The Bidder shall describe the methodology for end to end monitoring of the proposed solution / application through alerts and investigation of problem, issue through audit logs		
Tech-0141	Audit Trail and Logging	System must maintain an audit trail of all Administrative activities		
UI / UX				
Tech-0142	UI / UX	Platform should provide clutter free UI design with re-usable components and scalable open source modern UI library		
Tech-0143	UI / UX	Platform should provide responsive user interface which dynamically changes the platform appearance based on the size and orientation of the device being used		
Tech-0144	UI / UX	Needs to be simple, intuitive to reduce complexity and cognitive burden for the users		
Tech-0145	UI / UX	Needs to be consistent , by providing users with a sense of familiarity , so that their navigation and understanding of interface become easier		
Tech-0146	UI / UX	Needs to provide users with intuitive cues for their interactions with UI elements, so that they understand the outcome of their actions and feel in control with user interface		
Tech-0147	UI / UX	Needs to be accessible for all users including specially enabled ones by considering factors like font size, colour, contrast, keyboard navigation and screen reader compatibility		
Tech-0148	UI / UX	Needs to maintain a visual hierarchy of visual elements of screen to prioritize their importance and guide user's attention accordingly		
Tech-0149	UI / UX	Needs to provide clarity of the information and content by organizing content logically, using concise and straightforward language and using appropriate typography		
Tech-0150	UI / UX	Needs to provide appropriate error prevention and recovery mechanism by using necessary validations, informative error messages and intuitive error handling		
Tech-0151	UI / UX	System should provide for tool tips at each field and also online Help at the field level		
Tech-0152	UI / UX	System should display UI related errors encountered during transaction processing		
Tech-0153	UI / UX	Needs to provide adequate user control features by providing users the ability to navigate, interact and customize the interface as per their preference to enhance their ownership and engagement with the digital product they are using		
Tech-0154	UI / UX	Platform should provide optimum navigation design to achieve a. Reduced cognitive load on users b. Increased user engagement c. Enhanced user satisfaction d. Enhanced user content discovery abilities e. Reduced user bounce rate		
Database Requirements				
Tech-0155	Data Optimization and Performance	Database should support horizontal and vertical scalability to support future increase in transaction volumes and increase in number of concurrent users		
Tech-0156	Data Optimization and Performance	To support high availability and performance, system should support active/active as well as active/passive clustering. It should also support adding additional nodes to the cluster		
Tech-0157	Data Optimization and Performance	Should support tiering of data as per data availability and performance requirements. Most critical and frequently accessed data should be available in tiers which support high performance and so on.		
Tech-0158	Data Optimization and Performance	Should support compression tiering so that colder (Less frequently accessed) data is compressed to a greater level than actively accessed data in storage		
Tech-0159	Data Optimization and Performance	Reporting and analytical components of the platform should have separate environments to prevent delays and interruptions in operational environment		
Tech-0160	Back up and Restore	Service provider shall ensure a defined process for periodic backup		
Tech-0161	Back up and Restore	Should support parallel backup and recovery operations		
Tech-0162	Back up and Restore	Should support compressed backup		
Tech-0163	Back up and Restore	Support full, incremental and partial backups		
Tech-0164	Back up and Restore	Support full and partial recovery		
Tech-0165	Back up and Restore	Support point in time recovery		
Tech-0166	Back up and Restore	Support Auto-restart and recovery		
Tech-0167	Back up and Restore	Automatic/Manual tools for Back up and Recovery operations		
Tech-0168	Back up and Restore	Data Backup Plan: Platform should be capable of performing scheduled backup as per UIIC's policy.		
Tech-0169	Back up and Restore	Should support a backup and recovery plan to maintain the integrity and availability of the UIIC's information asset.		
Tech-0170	Back up and Restore	Should support a business continuity plan to maintain or restore operations and ensure availability of the UIIC's information asset as per UIIC's policy.		
Tech-0171	System Operation	The Bidder shall describe the archiving/back up mechanisms for database		
Tech-0172	Store and Archival	Should support set up of retention period for different types of data as per UIIC requirements/guidelines		
Tech-0173	Store and Archival	Should support manual/automatic archival of data as per defined intervals as per UIIC requirements/guidelines		
Tech-0174	Store and Archival	The system must support archival of data from the online transaction tables to History		
Tech-0175	Store and Archival	The system must support archival of data from History to offline		
Tech-0176	Store and Archival	The system must support managing compatibility of archived data for any table alterations as part of new releases.		
Tech-0177	Store and Archival	The archived data should be tracked and managed automatically, and the system should be able to retrieve archived data seamlessly in an online manner without specific user intervention.		
Tech-0178	Database security	Must adhere to Data localization norms and privacy protection norms as per UIIC's polices/Statutory and Regulatory requirements.		
Tech-0179	Database security	Should have Data Leak Protection capability which should allow setting security to ensure access to specific information only on validation of some critical fields at user level.		
Tech-0180	Database security	Authentication (adopt internationally accepted and published security standards that are not deprecated/ demonstrated to be insecure/ vulnerable)		
Tech-0181	Database security	Should support authentication of users		
Tech-0182	Database security	Encryption (adopt internationally accepted and published security standards that are not deprecated/ demonstrated to be insecure/ vulnerable)		
Tech-0183	Database security	Should support repository level as well as file level encryption/Decryption		
Tech-0184	Database security	Bidder and its solution must be adhere to UIIC's cloud and IS security policies/statutory/RBI/regulatory guidelines		
Tech-0185	Database security	Data at Rest - Service provider shall ensure that database encryption is in place		
Tech-0186	Database security	Platform to ensure Sensitive information like AADHAAR number and other PII information to be masked or encrypted in the database		
Tech-0187	Database security	Data masking and unmasking while interacting with various systems and webservices, wherever necessary		

Tech-0188	Database security	Complete Database level encryption		
Tech-0189	Database security	Database Column level encryption for PII/PCI compliance		
Tech-0190	Database security	Field level masking needs to be factored (presentation layer)		
Tech-0191	Database security	The database must support mirrored database solutions to have zero/minimal downtime.		
Tech-0192	Database security	The database must support real-time replication (Reporting,DR etc.)		
Tech-0193	Database security	The system should support data encryption at any field with the latest encryption technology based on pre-defined rules. This support should be available for all means of data entry e.g. manual through GUI / batch upload / interface etc., and should restrict display on front end, restricted reporting and encrypted storage in data warehouse etc. All business and transactional data is encrypted both in flight and at rest		
Tech-0194	Batch Jobs	Enable the operations to schedule a batch as well as a manual upload on an ad-hoc basis.		
Tech-0195	Batch Jobs	The system should allow the capability to accept encrypted data feed and process (with decryption at the system level).		
Tech-0196	Batch Jobs	Trigger a report to concerned user if a part of a scheduled set of activities (say certain programs/ activities) did not run as per schedule. These reports should be have capability to be auto emailed along with alerts (Email, SMS).		
Tech-0197	Batch Jobs	Allow a user to create a one time exception to the batch program (e.g. stop it running on a particular Friday but run it next Thursday). Capability with appropriate administrative controls and requisite audit trails logged.		
Tech-0198	Batch Jobs	The system should be able to monitor the performance of batch jobs based on the load at the time and allow for analysis of the optimum time and load to run the batch		
Tech-0199	Batch Jobs	A detailed report of all scheduled batch jobs in terms of no. of counts should be available. These reports should have capability to auto emailed along with alerts (Email, SMS).		
Tech-0200	Batch Jobs	System should provide report/dashboard at EOD/EOW/ EOM / EOY batch jobs with clear categorization of errors, show stoppers, alerts, performance reports, data transfer validations.		
Tech-0201	Batch Jobs	Batch jobs should be allowed to run under specific service id(s) and No transactions can be carried out with these service ids		
Tech-0202	Batch Jobs	System must have a dashboard for uploads which provide statistics such as batch details, count of accept/reject records, rejected records with reason and allow user to download these records.		
Tech-0203	Batch Jobs	Data validation rules to be configured through a GUI to validate against a range of values/specific value/master etc.		
Tech-0204	Batch Jobs	Details of rejected records with reports and reason for rejection at a record level		
Tech-0205	Batch Jobs	Allow re-upload/re-sending of corrected records		
Infrastructure				
Tech-0206	Environments	Solution must process all data within UIIC Cloud / UIIC provided or authorized Infrastructure. No data should go outside of UIIC operated / governed / approved data locations/cloud storage		
Tech-0207	Environments	Web, application, database components should be installed separately		
Tech-0208	Environments	The proposed solution should be capable to balance the load between multiple active instances. Bidder to explain how this is being achieved.		
Tech-0209	Environments	Bidder must be able to perform: implementing, configuring, deploying, and managing the Solutions/applications on the cloud environments		
Tech-0210	Environments	Ability to set up multiple environments which are: Development, SIT, UAT, Pre-Production, Production and Disaster Recovery (Near DR and Far DR)		
Tech-0211	Environments	Ability to configure Pre-Production on two separate instances (one for Pre-Prod - replica of Prod and one for Training - lower specifications)		
Tech-0212	Environments	The Bidder must address Common Vulnerabilities and Exposures (CVE) and audit observations as per the UIIC's requirement without any additional cost		
Tech-0213	Environments	As when required , the Bidder should address end to end setup of Product/Solution but not limited to maintenance/support activities such as installation,configuraton,upgrade, patch update, addressing of VAPT/Audit's observations, resolving technical/performances issues etc both at UIIC's SIT/UAT/DEV/Pre-PROD/Training and production environment (DC, DR site) without any additional cost to UIIC except AMC/ATS and cost of deployed resources(support personnel/developer) to UIIC.		
Tech-0214	HA, BCP & DR	Bidder to ensure a well defined and comprehensive Business continuity plan is in place including activities, roles & responsibilities which is agreed and signed-off with UIIC		
Tech-0215	HA, BCP & DR	During disaster, DR system should cover 100% demands as production during disaster		
Tech-0216	HA, BCP & DR	In the normal scenario, Bidder describe the way the configuration, log, configure parameters, or software are synchronized to other components (to HA and DR component).		
Tech-0217	HA, BCP & DR	The solution should be deployed on High availability architecture with minimum of following requirement; Bidder to explain how below will be achieved:		
Tech-0218	HA, BCP & DR	Component level High availability so that the server / instance will not be affected due to failure of one disk / power / processor		
Tech-0219	HA, BCP & DR	Node / instance level High availability so that the availability of the solution will not be affected due to failure of one Node / instances within the same DC.		
Tech-0220	HA, BCP & DR	Datacentre level High availability so that the availability of the solution will not be affected due to the unavailability / disaster situation at one Datacentre.		
Tech-0221	HA, BCP & DR	The new application/feature/patch/hotfix or any configuration changes should be synchronized across servers/instances having same function in DC and DR.		
Tech-0222	HA, BCP & DR	Solution should meet RTO - RPO and Availability requirement as per UIIC's policy/ requirement. Bidder should prove how solution can meet this requirement. For Far DR: - RPO: Less than 30 minutes - RTO: Less than 60 minutes For Near DR : Zero RPO and Near Zero RTO		
Tech-0223	HA, BCP & DR	Bidder should ensure continuity of operations in the event of failure of primary site and meet the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements. Setup Disaster Recovery (DR) site to take over the active role and route all requests through that site in case of failover.		
Tech-0224	HA, BCP & DR	DR drills are to be conducted once every calendar quarter, totalling four times per year		
Tech-0225	HA, BCP & DR	The bidder should configure and update a dashboard in the cloud platform to monitor RPO & RTO of each application and database in real time.		
Tech-0226	HA, BCP & DR	Bidder to ensure that during failover, near zero downtime for the applications and zero data loss during the switchover.		
Tech-0227	HA, BCP & DR	Bidder to ensure that during failover (DR) and BCP exercise, near zero downtime for the applications and zero data loss during the switchover and BCP exercise.		
Tech-0228	HA, BCP & DR	For RPO, recovery of data should include both Data at Rest and Data in Transit		
Tech-0229	HA, BCP & DR	Bidder to ensure that regular Sanity checks are performed in DR environments		
Tech-0230	HA, BCP & DR	Bidder should provide detailed DR playbook and Runbook (prior to the DR drill) including stakeholder communication plan, end to end activities for the Portal including functionalities, services, integrations etc.		
Build, Release & Environments				
Tech-0231	DevOps & DevSecOps	Ability to build DevOps/DevSecOps CICD pipeline by integrating the required tools		
Tech-0232	DevOps & DevSecOps	Ability for Build and Release should be automated using CICD Pipeline as per the provided technology stack		
Tech-0233	DevOps & DevSecOps	Ability to configure CICD pipeline to manage the release in all the environments listed above to ensure timely and automated deployments and manage any deviations in functionalities within the environments		
Tech-0234	DevOps & DevSecOps	Ability to rollback option in CICD pipeline in case the build fails in any of the environments		
Tech-0235	DevOps & DevSecOps	Ability to Integrate observability technical components within CICI Pipeline		
Tech-0236	DevOps & DevSecOps	In DevOps/DevSecOps pipeline, DR should be configured as one of the environments to maintain latest code, runtime components, libraries, configurations, data sync, required software upgrades		
VAPT				
Tech-0237	VAPT Assessment & Resolution	Ability to carry out VAPT audit of the functionalities developed and submit the report of VAPT findings to UIIC for each of the deployments/iterations going into Production		
Tech-0238	VAPT Assessment & Resolution	Ability to carry out VAPT audit of the functionalities developed and submit the report of VAPT findings to UIIC on Quarterly basis in case no major deployments are done in Production		
Tech-0239	VAPT Assessment & Resolution	Ability to carry out activities to address the findings of the VAPT Report / Audit findings and ensure all the findings are addressed and sign-off for the same is received from UIIC.		
Observability - to be provided as dashboard and MIS				
Tech-0240	API Executive Dashboard	Provide dashboard for a real-time overview of API performance across the solution, including • Platform APIs (APIs exposed by the platform) • Integration APIs (APIs consumed from external systems such as third-party entities and services)		
Tech-0241	API Executive Dashboard	Key Metrics to be tracked as part of the dashboard: •Overall, API Health Score •Total API Calls (Today / This Week) •Average Response Time •Error Rate % •Uptime %		
Tech-0242	API Key Usage Dashboard	Analyzes API usage patterns and highlights service preferences. •Weekly API Volume •Product Preference Trends •Customer Segmentation (by Age, Region, Income) •Insurer Integration Uptime		
Tech-0243	Transaction Monitoring	Captures end-to-end metrics of customer, policy, claims, servicing related transactions		

Tech-0244	Latency Trends	Provides visibility into performance degradation across different system components over time. Latency is tracked at multiple layers: •Application latency (internal): request processing, background jobs, DB queries. •Platform API latency: per endpoint, per service. •External API latency: integrations with 3rd-party services, payment gateways. •Network latency: CDN, load balancer, DNS resolution, cross-region hops. •Database latency: query execution, replication lag. •Cache latency: hit vs miss times (Redis ,Cache).		
Tech-0245	SLA Compliance Tracker	Ensures partners and services meet contractual service-level expectations. •SLA Targets vs Actuals •Breach Alerts •Monthly Compliance Summary •MFA Usage Trends •Consent Logs and Audit Trails		
Tech-0246	Observability Dashboard	System Performance & Availability •Overall uptime and availability by application, region, and environment. •Response time trends across critical user journeys •SLA/SLO adherence with comparison against defined error budgets.		
Tech-0247	Observability Dashboard	Data Flow and Integration Monitoring •Health of real-time and batch data pipelines. •API call success rates and latency for integration •Data synchronization status and reconciliation between internal and external systems.		
Tech-0248	Observability Dashboard	User Behaviour and Engagement Metrics •Active users (daily, weekly, monthly). •Funnel metrics (drop-offs, conversion rates across major workflows). •Performance impact on user satisfaction (latency vs bounce/abandonment).		
Tech-0249	Observability Dashboard	Monitoring health and availability of external API •Uptime, response latency, and error rates for partner and UIIC APIs. •SLA compliance tracking against committed targets. •Breach alerts and early warnings for dependency failures.		
Tech-0250	Exceptions and Security Alerts	Monitor exceptions and security alerts, triaged, and communicated to relevant stakeholders to maintain platform reliability, security posture, and compliance readiness.		
Tech-0251	Exceptions and Security Alerts	Sources of Exceptions & Alerts •Application Exceptions: Unhandled errors, failed transactions, service crashes. •Security Events: Authentication/authorization failures, suspicious login attempts, MFA bypass attempts. •Infrastructure Alerts: CPU/memory spikes, unauthorized access attempts, anomalous traffic patterns. •External Integrations: Failed or suspicious API interactions with partners, or third-party providers.		
Tech-0252	Exceptions and Security Alerts	Detection & Classification •Alerts generated via observability tools (e.g., CloudWatch, ELK etc). •Classified into Critical, High, Medium, Low severity levels.		
Tech-0253	Exceptions and Security Alerts	Communication & Notification Channels •Critical/High: Real-time notification via Email •Medium/Low: Logged in dashboard and included in weekly summary reports. •Audit Trail: All alerts automatically stored for compliance and governance review.		
Tech-0254	Predictive & Proactive Monitoring	Enables early warning systems and future trend analysis for operational resilience. •Anomaly Detection (sudden latency/errors) •Load/Traffic Forecasting (per service or endpoint) •Historical Trend Comparison •SLA/Latency Breach Prediction •Self-Healing Scripts/Auto-Remediation Hooks		
Tech-0255	Stakeholder-Specific Dashboards	Custom dashboards tailored to the visibility needs of different roles. CXO Dashboard: •Strategic KPIs (Success rate, transaction growth) •Geo Response Heatmaps •Business Impact Metrics		
Tech-0256	Stakeholder-Specific Dashboards	DevOps Dashboard: •Build/Deploy Pipeline Status •Count of rollback / rollback monitoring •Error Budgets & MTTR •Microservice Latency & Throughput		
Tech-0257	Stakeholder-Specific Dashboards	Infra/Network Dashboard: •System Health, CPU, Disk •DNS/FW Logs, Port Stats •Server Failover & Uptime Trends		
Tech-0258	ICR/OCR	Solution must provide dashboards and MIS for monitoring OCR/ICR accuracy, processing turnaround time, and exception volumes.		
Compliance				
Tech-0259	Information Security Compliance	Ability to address any VAPT findings that UIIC may raise with them emerging from their own VAPT audit or from third party as per UIIC's discretion		
Tech-0260	UIIC Guidelines/Policies Compliance	Ability to comply with: Information and Cyber Security Policy (ICSP) – UIIC internal policy Policy on Physical and Environmental Security – UIIC internal policy Policy on Asset Management – UIIC internal policy Policy on Information Systems Acquisition and Development – UIIC internal policy Policy on Information Systems Maintenance – UIIC internal policy Cloud Security Alliance (CSA) – Cloud Controls Matrix (CCM)		
Tech-0261	Regulatory & Industry benchmarking Compliance	Ability to comply with: ISO/IEC 27001:2013 – Information Security Management Standard IRDAI Guidelines on Information and Cyber Security – As applicable to insurance entities MeitY Guidelines on Adoption of Cloud Services – Government of India		
Specific Technology Component - Technical Requirements				
Tech-0262	Conversational Bot Platform	Platform should provide a GenAI based chatbot which is available 24/7 for any service request and provides conversational experience using NLP		
Tech-0263	Conversational Bot Platform	Platform solution should be able to handle minimum 10,000 concurrent Chat Sessions		
Tech-0264	Conversational Bot Platform	Platform solution should be able to provide minimum conversation response accuracy of 95%		
Tech-0265	Conversational Bot Platform	Platform solution should be able to handle minimum chatbot uptime of 99.50% on quarterly basis.		
Tech-0266	Conversational Bot Platform	Platform should have capability to send communication on WhatsApp , SMS and e-Mail for internal and external communication		
Tech-0267	Conversational Bot Platform	The functionality of ConversationalBots features exposed for external consumer as API.		
Tech-0268	Conversational Bot Platform	Fallback Count Percentage of user response that the Bot could not comprehend or comprehended incorrectly. For 1st Year after Go-Live - Should be less than 20%		
Tech-0269	Conversational Bot Platform	Fallback Count Percentage of user response that the Bot could not comprehend or comprehended incorrectly. After 1 Year after Go-Live - Should be less than 10%		
Tech-0270	Conversational Bot Platform	Drop off rate Percentage of user interactions that are not responded to by the Bot. (excluding external factors like API response from UIIC etc.). For 1st Year after Go-Live - Should be less than 10%		
Tech-0271	Conversational Bot Platform	Drop off rate Percentage of user interactions that are not responded to by the Bot. (excluding external factors like API response from UIIC etc.). After 1 Year after Go-Live - Should be less than 5%		

Tech-0272	Conversational Bot Platform	The Platform should have capability to connect to other platforms/systems through APIs, Webhooks etc. and connect with UIIC Systems as made available by UIIC.		
Tech-0273	Conversational Bot Platform	The platform shall also be capable of connecting to any third-party platform to enhance the service offerings to the end user through Bot.		
Tech-0274	Conversational Bot Platform	The platform should be able to integrate with any other in-house/ticketing tool that UIIC may wish to introduce for logging tickets that require UIIC servicing team intervention.		
Tech-0275	Conversational Bot Platform	For outbound conversations like (broadcasting reminders, status updates etc.) the platform should be able to integrate with UIIC's Call Center Dialler .		
Tech-0276	Conversational Bot Platform	Platform should be able to integrated with UIIC's SMS and Email Gateways for sending communications over SMS and Email to the customer (example – feedback surveys)		
Tech-0277	Conversational Bot Platform	Platform to support customization of Reports and Dashboards based on available parameters		
Tech-0278	Conversational Bot Platform	Platform must comprise of an interactive dashboard containing detailed MIS		
Tech-0279	Conversational Bot Platform	**Measurability -** Platform should provide the metrics and transparency to monitor the efficiency of the Chatbot. Few key parameters like Interactions per User, Average Daily Sessions, Goal Completion Rate (GCR), Customer Satisfaction Rate, Confusion Rate, Chat Reset, Human Takeover Rate (Triggered by Repeat Fails), etc		
Tech-0280	Conversational Bot Platform	Platform to support extraction of standard reports in PDF and also be exportable to Word or Excel or other data analysis formats		
Tech-0281	Conversational Bot Platform	Platform to support runtime extraction of reports and scheduled reports for various stakeholders across organisation.		
Tech-0282	Conversational Bot Platform	Customer Analytics and Bot Behaviour Analysis: Platform should be able to capture customer information such as email-id, IP address, browser/OS details etc. and relevant data as applicable / required by UIIC for data analysis. Solution should provide dashboard with real-time statistics and historical reports on Conversational Bot executions. Platform to provide statistics on its ability to respond to user commands or queries in the shortest amount of time and best way possible.		
Tech-0283	Conversational Bot Platform	Platform should be capable of providing chat volumes, response time to chat requests, lead time to resolve the query, customer related information, Conversational Bot availability report (uptime/downtime), other reports as per business user requests.		
Tech-0284	Conversational Bot Platform	Platform to provide standard reports like concurrency, licenses consumed, etc.,		
Tech-0285	Conversational Bot Platform	Capability to generate user and conversation-level reports, including but not limited to: • Total users, active users, engaged users, new users, average number of conversations per user, users' demographics wise distribution, sessions per day, user feedback rating etc. • Conversation Starter Messages: Count of sessions where the Bot started the conversation with user • Total Bot Interactions: Count of total messages sent by the bot in each interactive session • In Bound Messages: Count of total messages sent by the user in each interactive session • Fallback counts: Number of unprocessed messages by the Bot • Success Count: Number of successfully completed conversations • New Conversations: Total number of new conversations started by the user, either returning user of the bot or a new user.		
Tech-0286	Conversational Bot Platform	Capability to track bot KPIs, including but not limited to: • User Retention: The number of users returning to the bot in a given period of time • Dashboard with real-time usage statistics • Response Time: Bot's response time (average, min, max etc) • Fallback rate: This would capture Bot's failure in delivering service to user. • User Satisfaction: A matrix defined through exit surveys of the users interacting with the bot. The users should be given the option to rate the Bot's service and an optional description of the issue if any. • Bot Availability: Uptime / Downtime • Word to Error Ratio: There should be a report that shows the 'word to error ratio' of the solution. (Error ratio means the ratio of no. of correctly identified words by Bot to the words that were not correctly identified).		
Tech-0287	Workflow	System shall have capabilities to have seamless integration with external workflow system		
Tech-0288	Workflow	System should be able to have both inward and outward integration with respect to task performance and updation to external workflow system.		
Tech-0289	Workflow	Solution should be able to host, maintain and use a role-rights hierarchy assigning privileges on functionality to different types of internal and external users of UIIC		
Tech-0290	Workflow	Solution should have a capability to generate, maintain and publish transaction status in the workflow with identification of user attending and record date/time stamp of events.		
Tech-0291	Middle Office Layer	The solution should provide out of box product templates, formulae which would accelerate the product definition		
Tech-0292	Middle Office Layer	Solution should have provision to create product libraries for different lines of product example Motor, Marine, Health, Commercial Lines etc		
Tech-0293	Middle Office Layer	Solution should support fulfilment of transaction on this layer with minimum or no dependency on the core system		
Tech-0294	Middle Office Layer	There should be a provision to extend this layer to integrate with new and other core systems within the eco system of UIIC		
Tech-0295	Middle Office Layer	Solution should have development Tool for defining new services and also integration with up stream and downstream systems		
Tech-0296	Middle Office Layer	Should support Service Based / File Based integration options for Downstream Data Sync		
Tech-0297	Middle Office Layer	The solution should have a transformation layer for data transformation/enrichment as excepted by the destination application while receiving data from multiple sources (Partner, OEM and internal systems) to facilitate the completion of transaction		
Tech-0298	Middle Office - product configurator	The solution should have capability of complete product management in terms of version control & allow product cloning		
Tech-0299	Middle Office - product configurator	Solution should have Graphical user interface to define product related attributes		
Tech-0300	Master Management	Ability to create and maintain masters to support functional modules such as New business, Endorsement activity, Claims etc. (as per the scope of the RFP)		
Tech-0301	Master Management	Ability to support creation and modification of all masters required through GUI, changes , audit trail should be maintained for the changes in the masters		
Tech-0302	Master Management	Ability to support versions of master with effective date and expiry date of versioning. All such versions should be stored for audit trail and applicability to respective transactions.		
Tech-0303	Master Management	Ability to upload new/modifications to master through an xls, csv,flat file etc. Also, the REST/SOAP service should be exposed to external system to create and modify master data		
Tech-0304	Master Management	The system must allow to query, fetch or update master record through API's		
Tech-0305	Content Management System	Bidder should be responsible for configuration of new Content Management System (CMS) at the Primary and Disaster Recovery site		
Tech-0306	Content Management System	Bidder should handle Migration of the existing content to the new CMS		
Tech-0307	Content Management System	Bidder should handle Configuration of users, groups and workflow for various stakeholders of UIIC on the CMS for content authoring and publishing approval.		
Tech-0308	Content Management System	Bidder should provide for the Configuration of content authoring workflows		
Maintenance				
Tech-0309	Maintenance	Bidder to ensure that proposed solution will use the latest available technology stack and incorporate all recent improvements in design, scalability, performance, and security.		
Tech-0310	Maintenance	Bidder to ensure that no component within the solution suffers from defects due to architectural design, integration issues, or operational inefficiencies under normal usage		
Tech-0311	Maintenance	Bidder shall have a defined process towards periodic patching to be conducted for OS, DB, Application, Web Server, any additional servers, network & security devices in scope		
Non-Functional Requirements (NFRs)				
NFR-0001	Accessibility	Capability should be available in the platform to enable accessibility features based on future requirements		
NFR-0002	Accessibility	Will support all major screen reader software		
NFR-0003	Accessibility	The solution should be accessible from multiple channels, such as, but not limited to, desktop, mobile, etc.		
NFR-0004	Accessibility	Linkage to document storage system and retrieval		
NFR-0005	Accessibility	Bidder should comply with GIGW 3.0 & WCAG 2.1 guidelines for accessibility related regulatory guidelines for all user facing assets including portals/ mobile app / microsites etc.		
NFR-0006	Accessibility	Bidder should attain STQC certifications for all website/portal/mobile apps and share with UIIC when required		
NFR-0007	Accessibility	Bidder should comply with all regulatory essential pre requisites of the useable, user centric and universal accessible (UUU trilogy)		
NFR-0008	Auditability (Audit and logging)	Audit trails need to be available for users accessing services to view or read information		
NFR-0009	Auditability (Audit and logging)	The solution should have the functionality to determine details of a change and about the users making the change and the date and time of making the change.		
NFR-0010	Auditability (Audit and logging)	The solution should capture IP Address, location details etc. to identify the source of event/transaction		
NFR-0011	Auditability (Audit and logging)	Solution shall capture full audit trails, audit logs and transaction logs (what, when, who has changed), comprehensive admin activity logging		
NFR-0012	Performance & Scalability	System should be able to scale in order to meet business volumes of UIIC		
NFR-0013	Performance & Scalability	System should support operations on a 24*7 basis ensuring availability of Solution/Platform, integrations and other components		
NFR-0014	Performance & Scalability	Platform should be highly available, resilient and with zero downtime and zero data loss target		
NFR-0015	Performance & Scalability	The solution must have the ability to recover from bad data (auto data recovery) and out-of-range or invalid commands automatically, without resulting in a system crash.		
NFR-0016	Performance & Scalability	Support deployments with load balanced models(such as requests from load balancer to web server to application server)		
NFR-0017	Performance & Scalability	The solution should be scalable, both vertically and horizontally based on server load or number of transactions and with respect to new user requirements		
NFR-0018	Performance & Scalability	The solution and its components must fully support and planned to be explicitly configured for stateless architecture to enable on-demand scalability and elasticity		
NFR-0019	Performance & Scalability	Capacity to carryout high-volume transactions with optimum response time and performance		
NFR-0020	Performance & Scalability	The bidder should be responsible for continuous monitoring of the performance post launch and gather feedback for improvements		
NFR-0021	Performance & Scalability	System CPU utilization should not exceed 60-70% during peak load to ensure optimal performance.		
NFR-0022	Performance & Scalability	Memory usage should remain within 70-75% during peak periods to avoid performance bottlenecks.		
NFR-0023	Performance & Scalability	Comprehensive load testing must be performed to ensure the system can handle peak load conditions effectively.		
NFR-0024	Performance & Scalability	The solution must support dynamic, auto-scaling of resources based on real-time demand, triggering only when system-utilization thresholds exceed the defined limits		
NFR-0025	User facing Assets - Performance	Time to Title - Time elapsed when a browser/app downloads the first byte on the Platform and the solutions' title displays in the browser/app: Should be less than 1300ms		
NFR-0026	User facing Assets - Performance	Time to Start Render - Time elapsed when the first visible element appears on the blank page: Should be less than 2500ms		
NFR-0027	User facing Assets - Performance	Time to Display - Time elapsed when all visual elements of the page are in place: Should be less than 5000ms		

NFR-0028	User facing Assets - Performance	Time to Interact - Time elapsed when a user has gained control of a webpage and can interact with content: Should be between 4000ms to 6000ms		
NFR-0029	Extensibility	The solution should support addition of new features and technologies as and when needed in the future		
NFR-0030	Extensibility	New enhancements should not be made by impairing existing functionalities		
NFR-0031	Compatibility	The solution should support multiple platforms, such as, but not limited to, Windows, Linux, Android, iOS, etc.		
NFR-0032	Compatibility	The solution should allow to be accessed from different web browsers, such as (not limited to) Chrome, Edge, Safari, and Firefox		
NFR-0033	Compatibility	The solution should support all industry standards interfaces for interoperability with other systems in UIIC environment		
NFR-0034	Compatibility	Capability to configure to existing modules, add new modules and have enough flexibility to accommodate changes in schemes and products		
NFR-0035	Compatibility	Capability of backward browser/ device compatibility to continue for external facing functionalities		
NFR-0036	Fault Tolerance	The solution shall be robust enough to continue operation despite an invalid data input, instead of crashing completely		
NFR-0037	Fault Tolerance	On any deviation from expected outcome, system should continue functioning fully operational with, perhaps, a reduction in throughput or an increase in response time		
NFR-0038	Fault Tolerance	Fault isolation to the failing component – When a failure occurs, the system must be able to isolate the failure to the offending component		
NFR-0039	Fault Tolerance	The solution shall implement zero fault tolerance; for certain errors, generate notifications and critical errors should trigger alerts via SMS/E-mail to designated users.		
NFR-0040	Deployability	The bidder should have isolated development/test environments from other environments (such as production) and internet ensuring a clear separation of access controls		
NFR-0041	Deployability	Making deployment straightforward, low-risk and Push-button event.		
NFR-0042	Security And Logging	The system should ensure that the personal information of the users is secure and should comply with regulations		
NFR-0043	Security And Logging	Handle all customer PII data carefully by not logging it and masking whenever it is applicable		
NFR-0044	Security And Logging	Platform must be protected from un-authorized access		
NFR-0045	Security And Logging	Platform must provide end-to end encryption for data in-transit using TLS 1.3 and for in-rest using 256 bit AES		
NFR-0046	Security And Logging	Robust security monitoring and logging mechanisms to detect and respond to security incidents. Collect and analyse security logs to identify potential threats or breaches in real-time.		
NFR-0047	Security And Logging	The solution must include the capability to log and monitor API calls, providing comprehensive visibility and auditability of all API interactions		
NFR-0048	Security And Logging	Platform must be resilient to any kind of attacks including DDOS and XSS attacks		
NFR-0049	Security And Logging	Platform must manage logging centrally with appropriate log aggregator design		
NFR-0050	Session and State Management	Service provider's solution must adhere to the following: i. Session Time - As per UIIC requirements (to be provided later to the successful bidder) ii. Session Traffic must be encrypted using strong crypto algorithm which are not deprecated/ demonstrated to be insecure/ vulnerable		
NFR-0051	Session and State Management	Platform should define session time out in case the user does not use the application for the defined time limit		
NFR-0052	Session and State Management	Platform should manage session data diligently with combination of Cache and database		
NFR-0053	Search Capability	The capability to define the mandatory fields for optimal search results and to configure the results returned (limit to minimize DB issues etc.)		
NFR-0054	Search Capability	Capability to be provide configurable search screen based on user security allowed (E.g. Specific users can view customer sensitive information like PAN card)		
NFR-0055	Search Capability	Capability to configure the search fields (that are available in the Platform) on the search page without code level changes		
NFR-0056	Multilingual Support	Front end portals (Website, Customer Portal, Agent Portal and respective apps) should multiple languages (as per the scheduled languages of the Government of India)		
NFR-0057	Localization	The solution must use agreed local formats for dates, addresses, and phone numbers		

B. Integration Requirements			Bidder Response	Remarks
S. No	Area	Requirements		
Integration				
IR - 1	Integration Requirements	Platform should provide capabilities to integrate with UIIC Systems and services including but not limited: Genesys Configurator - Core Insurance Solution OmniDocs DMS SAP - Finance System NEFT Portal (Payouts) NEFT Portal (Receivable) RCSC Claims Portal Intranet Unified Grievance Management System Exadata Emailing Solution SMS Service SAP HRMS Corporate Website Customer Portal/PWA Distributor App | Portal Surveyor Portal VAIS Portal Payment Gateway Email Gateway SMS Gateway		
IR - 2	Integration Requirements	Platform should provide capabilities to integrate with external third party services including but not limited: UIDAI KYC NSDL GST/ PAN IIB Vahan EKYC Account Aggregator ABHA Jan Suraksha ETASS Penny Drop EIA (ITrix) AHD NCHX Digi locker ABDM ENACH IRDAI		
IR - 3	Integration Requirements	Platform should provide capabilities to integrate with external third party entities including but not limited: Brokers Brokers OEM/MISP Web aggregators Affiliates Garages TPA CSC Webster		
Integration - Technical Requirements				
IR - 4	Platform Integration	Describe the supported type of integration for Application and Data Integration (real-time, batch, MQ, Web Service, ESB,API, etc...)		
IR - 5	Platform Integration	The System shall support message based collaboration based on standard network protocols but not limited to HTTPS, SFTP and SMTP (Secure)		
IR - 6	Platform Integration	The System shall support SMTP based integration with Email Servers.		
IR - 7	Platform Integration	Platform to support Integration using APIs, ISO, Web services, ESBs, MQs, Custom Adapters, pre-built integrations with backend systems etc.		
IR - 8	Platform Integration	Platform should have a common wrapper layer built using best practices and standard protocols for all API interactions where data transformation is required		
IR - 9	Platform Integration	Ensure seamless integration between Platform and other applications by adhering to industry standard protocols and data formats		
IR - 10	Platform Integration	Platform to support Fine grained Integrations for services (no need for message mediation, transformation, choreography etc.)		
IR - 11	Platform Integration	Platform to support Coarse grained integration for services (service is calling another service, requiring message mediation, transformation, choreography etc.)		
IR - 12	Platform Integration	Ensures data remains accurate and reliable across different systems by using techniques like data validation, duplication check and referential integrity		
IR - 13	Platform Integration	Gracefully handle and recover from failure by implementing strategies like exception handling and appropriate failover mechanisms		
IR - 14	Platform Integration	Platform integrations should be designed for easy maintenance and adoptability to future changes in technology and business requirements		
IR - 15	Platform Integration	Platform integrations should adopt to security first features like robust encryption, access control and regular security audits to handle secured data flow across the systems		
IR - 16	Platform Integration	Platform integrations should scales up or down based on the demand ensuring performance and stability under varying loads		
IR - 17	Platform Integration	All subscribers to platform's APIs need to be whitelisted and registered on API gateway		
IR - 18	Platform Integration	All consumptions of external services by platform will be through ESB layer		
IR - 19	Platform Integration	The system should act as a broker between systems to allow for real time streaming of data and exchange of information		
IR - 20	Platform Integration	The system should be able to relay messages between producers and consumers.		
IR - 21	Platform Integration	The system should be highly available, clustered and highly distributed		
IR - 22	Platform Integration	The system should have excellent business continuity		
IR - 23	Platform Integration	The system should be able to identify if a message from single producer needs to consumed by multiple consumers and vice versa. The system is expected to be intelligent enough to store the data for relevant time periods by all relevant recipients		
IR - 24	Platform Integration	The system should be able to identify a pattern of requests and accordingly, effectively optimize their response time for a work queue or department		
IR - 25	Platform Integration	The system must have standards Support – WSDL, XML, XSD, XSL, JSON, REST, Digital Signatures, OAuth, SAML, JWT		
IR - 26	Platform Integration	System should support TLS 1.1, TLS 1.2 and TLS 1.3 to offer strict security requirements		

IR - 27	Platform Integration	The solution must include support for legacy encryption protocols to accommodate integrations that utilize older TLS encryption standards.		
IR - 28	Platform Integration	System should have data mapping for transforming XML, text, JSON, transaction management (Automatic, Commit, Rollback)		
IR - 29	Platform Integration	System should have support for standard scripting languages		
IR - 30	Platform Integration	System should have connectivity and integration to Databases, JEE applications, FTP servers, JMS, and messaging services like (MQ,Kafka)		
IR - 31	Platform Integration	The system should be able to perform workload management		
IR - 32	Platform Integration	The architecture will follow both the microservice design principles of autonomous services and ESB capabilities of loosely coupled functional units and infrastructure to provide UIIC with a robust and agile integration platform to meet their enterprise needs		
IR - 33	Platform Integration	Enterprise service policy definition and enforcement – A single repository shared among the agencies with governance framework. Helps achieve naming standards, identify the master systems for services and critical data elements like unique identifier		
IR - 34	Platform Integration	The system must provide Orchestration and club fine grained components into a single business service. The components could be any legacy systems and distributed systems		
IR - 35	Platform Integration	The system must manage relationships between loosely coupled and uncoupled business components and expose them as a Business Service		
IR - 36	Platform Integration	The system must support interactions from source to target such that the source and target can only interact with ESB and do not have to interact with each other		
IR - 37	Platform Integration	The system must provide for a centralized location to discover and access the services		
IR - 38	Platform Integration	The system must isolate the applications from detailed knowledge of the services, allowing for change in the description of a service in one location, without having to update any dependant applications		
IR - 39	Platform Integration	The system should be able to handle exceptions and handle exception logging mechanism		
IR - 40	Platform Integration	The solution must include support for legacy encryption protocols to accommodate integrations that utilize older TLS encryption standards.		
IR - 41	Platform Integration	System should provide APIs for interacting with other systems.		
IR - 42	Platform Integration	System should be able to integrate with middleware environments.		
IR - 43	Platform Integration	System should be able to integrate with BPM and workflow products		
IR - 44	Platform Integration	The system should be able to interact with other back office systems		
IR - 45	Platform Integration	The system must support both online(xml,web-services) and batch based interface unidirectional or/and bi-directional.		
IR - 46	Platform Integration	Configuration of the feed file including field definition (Field sequence, length, data type, mandatory/optional etc) should be configurable through a GUI. System should validate the file format and parse the format.		
IR - 47	Platform Integration	System must provide the log for web-service interaction (Request and response time, Payload, Success/failure status etc.)		
IR - 48	Platform Integration	The sensitive client information must be masked/encrypted in the interface files.		
IR - 49	Platform Integration	Solution should be capable of integrating with any new/future system that UIIC may develop in the future. The requirements for the integration will be discussed with the vendor for integration		

C. Cloud Requirements				Bidder Response	Remarks
Sr no	Category	Area	Description		
A. Regulatory and Compliance Requirements					
1	Regulatory / Security/ Compliar	Conformance to Regulations	Should be empanelled with **MEity**		
2	Regulatory / Security/ Compliar	Conformance to Regulations	Preferable to have **GCC (Government Community Cloud) compliance** by adhering to regulatory standards for security, privacy, and data sovereignty specific to government entities.		
3	Regulatory / Security/ Compliar	Conformance to Regulations	Vendor to ensure that UIIC data related to the portal (including any data in transit or at rest) is **restricted** to remain within the **geographical boundaries of India**.		
4	Regulatory / Security/ Compliar	Conformance to Regulations	Ensure **compliance** with guidelines and certifications from **regulatory authorities**, confirming that the UIIC's data will reside in Data Centers located in India.		
B. CSP Related Requirements					
1	Cloud Service Providers Capabil	CSP Profile	Provide comprehensive details of the CSP's platform and the various services offered.		
2	Cloud Service Providers Capabil	CSP Profile	The CSP should establish a clearly defined multi-year roadmap for its cloud services in India.		
3	Cloud Service Providers Capabil	CSP Profile	The CSP must ensure that all features and services available for the India region, including AI capabilities, are clearly listed on their website. Furthermore, the CSP should utilize hardware optimized for AI to effectively support these capabilities		*<Bidder to provide relevant link>*
4	Cloud Service Providers Capabil	CSP Profile	The CSP should publish the rates for all services offered in India in Indian currency on their website.		*<Bidder to provide relevant link>*
5	Cloud Service Providers Capabil	Cloud Provider Technical Support	Describe implications of managed services on customer engagement with CSPs, including support agreements between MSP and CSP for 2nd and 3rd tier **incident resolution**.		
6	Cloud Service Providers Capabil	Accreditations/Certifications	Provide details of Accreditations/Certifications of Cloud Service Providers, along with a complete business profile, including duration in the cloud service business and core strengths.		
7	Cloud Service Providers Capabil	Networking Services	Provide complete network details and requirements for data flow within the CSP, connections between CSP and UIIC premises, and network diagrams for onboarding applications.		
8	Cloud Service Providers Capabil	Architecture Services	The CSP should provide Architecture advisory services such as Azure Advisory Services and the AWS Well-Architected Framework etc.		
9	Cloud Service Providers Capabil	Architecture Services	The CSP should have availability of different tier of managed Object storage service including class/tier that intelligently and automatically migrates data between classes/tiers based on usage pattern of the objects in the storage and ability to scale IOPS and throughput of high performance block storage independent of storage capacity.		
10	Cloud Service Providers Capabil	CSP Profile	Bidder to submit the Following Specifications for each of the environments mentioned in the RFP • Landing Zone Architecture Diagram • Platform Solutions Architecture Diagram • Network Diagram (indicative) • Details of all proposed software specification along with OEM and features of each software platform • Proposed internal and external network specification • Security Controls and Mechanisms • Any other relevant artefacts		
11	Cloud Service Providers Capabil	CSP Profile	CSP should be able to maintain Active-Active setup for DC & Near DR AND Active-Passive setup for DC and Far DR		
12	Cloud Service Providers Capabil	CSP Profile	CSP should have the capability to provide both high availability and Near DR from two or more physically isolated (by minimum of 10 kilometres) MeitY empanelled data centre sites within a single region supporting synchronous replication		
13	Cloud Service Providers Capabil	CSP Profile	CSP should have the capability to provide synchronous data commit in Near DR from DC to ensure high availability in a cost effective way		
14	Cloud Service Providers Capabil	CSP Profile	CSP should have the capability to provide snapshot based data replication from DC to Near DR in a cost effective way		
15	Cloud Service Providers Capabil	CSP Profile	CSP should have the capability to provide a far DR in a different seismic zone from the Primary DC and/or near DR sites.		
16	Cloud Service Providers Capabil	CSP Profile	CSP should have capability to offer Zero RPO and Near Zero RTO for Near DR and maximum 60 Minute RTO and 30 Minute RPO for Far DR		
17	Cloud Service Providers Capabil	CSP Profile	CSP should have the capability to provide zero data loss (transaction, documents) during the switchover (during failover and BCP/DR drill)		
18	Cloud Service Providers Capabil	CSP Profile	CSP should declare the locations (cities) for Availability Zones, Regions etc. that are proposed as part of the solution.		
C. Landing Zone Requirements					
1	Landing Zone	Foundation / Infrastructure	The design phase will involve collaboration between UIIC and the vendor. The vendor will provide guidance and recommendations based on best practices, while UIIC will make the final design decisions and approve the design prior to implementation.		
2	Landing Zone	Foundation / Architecture Setup	Provide comprehensive details and design for landing zone creation, including estimated costs and time involved.		
3	Landing zone	Foundation / Architecture Setup	Establish a **Resource Group (RG), Virtual Network (vNet)/VPC (Virtual Private Cloud)/any other similar Virtual network mechanism** for cloud service deployment.		
4	Landing zone	Foundation / Architecture Setup	**Configure subnets** in alignment with the architecture diagram.		
5	Landing zone	Foundation / Architecture Setup	Create **management groups or organizational units** to establish a clear **resource hierarchy** within the cloud environment		
6	Landing zone	Foundation / Architecture Setup	Structure subscriptions, accounts, or projects based on specific workload needs, **ensuring optimal resource allocation and management**		
7	Landing zone	Foundation / Architecture Setup	Manage **licensing requirements** for cloud resources, ensuring compliance with software and service agreements within the landing zone		
8	Landing zone	Foundation / Architecture Setup	Setup of **Development, User Acceptance Testing (UAT), SIT, Pre-Production, and Production** Environments		
9	Landing zone	Foundation / Architecture Setup	All the above environments, VPCs and data should be within India Region ensuring that no data is exposed outside of India boundary.		
D. Network					
1	Networking Services	Foundation / Infrastructure	Deploy and set up **Cloud Application Gateway** for effective load balancing.		
2	Networking Services	Foundation / Infrastructure	Activate **Web Application Firewall** (WAF) to safeguard against common vulnerabilities such as SQL injection and XSS.		
3	Networking Services	Foundation / Infrastructure	Establish **load balancing rules** and implement **SSL termination** for secure communication		
4	Networking Services	Foundation / Infrastructure	Establish best practice usage of multiple availability zones within the cloud environment to ensure high availability and resilience.		
5	Networking Services	Foundation / Infrastructure	Establish Active-Active setup for DC & Near DR AND Active-Passive setup for DC and Far DR		
6	Networking Services	Foundation / Infrastructure	Establish either synchronous data commit in Near DR from DC or snapshot based data replication from DC to Near DR to ensure high availability in a cost effective way as per the proposed solution		
7	Networking Services	Foundation / Infrastructure	Establish far DR in a different seismic zone from the Primary DC and/or near DR sites.		
8	Networking Services	Foundation / Infrastructure	Establish the capability to offer Zero RPO and Near Zero RTO for Near DR and maximum 60 Minute RTO and 30 Minute RPO for Far DR		
9	Networking Services	Foundation / Infrastructure	CSP should have the capability to provide zero data loss (transaction, documents) during the switchover (during failover and BCP/DR drill)		
10	Networking Services	Foundation / Infrastructure	CSP should declare the locations (cities) for Availability Zones, Regions etc. that are proposed as part of the solution.		
11	Networking Services	VPN	Bidder to provide application/tool (VPN) to enable integration between UIIC system/peripherals (on-prem) with cloud resources in DC. UIIC prefers fastest VPN (such as express route) and capability of fastest possible data transfer between applications of UIIC systems/peripherals and cloud resources.		
12	Networking Services	VPN	Bidder should provision for VPN to allow UIIC designated IT spocs to access cloud resources.		
E. Cloud Management Platform					
1	Cloud Management Platform	Foundation / Management Layer	Provide a high-level overview of the cloud management platform and integrated tooling used for service delivery, including details on third-party CMP components.		
2	Cloud Management Platform	Foundation / Management Layer	Implement **data synchronization policies** across multiple environments		
3	Cloud Management Platform	Foundation / Management Layer	Establish **data retrieval policies** that define access controls and procedures, ensuring security and compliance with UUIC standards		
4	Cloud Management Platform	API Management	Deploy **API Management** for managing, publishing, and securing APIs		
5	Cloud Management Platform	Service Layer / Application	The vendor to develop the application, ensuring that all application rights, source code, and related assets are owned by UIIC		
6	Cloud Management Platform	Service Layer / Storage	**Create and configure Storage Accounts** for the purpose of storing unstructured data in Blob Storage		
7	Cloud Management Platform	Service Layer / Storage	CSP should be able to offer file storage with multi-attach capability to attach a single volume to multiple compute instances for shared access, ideal for clustering/high availability apps.		
8	Cloud Management Platform	Service Layer / Storage	CSP should have the ability to do dynamic Online Volume Modification with the ability to support resizing volumes, changing volume types, and adjusting performance parameters on the fly without downtime.		

9	Cloud Management Platform	Service Layer / Storage	All the services enabled on the cloud for this solution / services of cloud provider leverage for this solution should be configured within India only		
10	Cloud Management Platform	Service Layer / Data	Provision Cloud Database for SQL in accordance with the Bill of Materials (BOM)		
11	Cloud Management Platform	Configuration Management	Describe services that ensure and maintain configuration standards, capable of preventing, detecting, and remediating configuration changes, including **policy-based controls, actionable events, automated workflows, and reporting**.		
12	Cloud Management Platform	Hybrid Management and Customer Infrastructure Integration Services	Provide information on **management capabilities** addressing hybrid requirements, identity and access management solutions, and integration of workloads and infrastructure in on-premise and hosted solutions.		
F. DevOps/DevSecOps					
1	Cloud DevOps	CI/CD & Development Operations	Enable **Cloud DevOps Organization** and integrate it with the subscription through a **Service connection**		
2	Cloud DevOps	CI/CD & Development Operations	Configure CI/CD pipelines for deploying services in Production App Services		
3	Cloud DevOps	CI/CD & Development Operations	Ability to provide options for automating resource deployment using DevOps practices.		
4	Cloud DevOps	Provisioning, Orchestration, and Automa	Provide an overview of **managed services** for the creation, deletion, modification, and orchestration of cloud assets.		
5	Cloud DevOps	Provisioning, Orchestration, and Automa	Utilize **automation tools** to streamline repetitive tasks and orchestrate **complex workflows**		
6	Cloud DevOps	Provisioning, Orchestration, and Automa	Implement **CI/CD pipelines** for continuous integration and deployment		
7	Cloud DevOps	Provisioning, Orchestration, and Automa	Automate the setup of a secure baseline cloud environment with central governance through Landing Zone Setup.		
8	Cloud DevOps	Provisioning, Orchestration, and Automa	Ability to offer options for automation tools to address ongoing and business-as-usual (BAU) management tasks.		
9	Cloud DevOps	Provisioning, Orchestration, and Automa	Ability to configure resource management solutions for on-premises and cloud workloads using hybrid management tools.		
G. Monitoring & Analytics					
1	Monitoring and Analytics	Operations / Monitoring	Specify services for **tracking and reporting** on the availability, health, and performance of deployed infrastructure, leveraging monitoring and analytics for self-healing and automation, along with recent successes.		
2	Monitoring and Analytics	Operations / Monitoring	Bidder shall ensure ongoing health, performance, and availability of the cloud infrastructure provisioned for the platform.		
3	Monitoring and Analytics	Operations / Monitoring	Bidder shall utilize appropriate cloud-native monitoring and incident response tools to proactively track system health, performance, and fault occurrence metrics. These should be shared with UIIC periodically as part of governance and audit		
4	Monitoring and Analytics	Operations / Monitoring	Continuously **monitor** the **performance** and **utilization** of cloud resources and applications		
5	Monitoring and Analytics	Operations / Monitoring	Track metrics and logs for performance and utilization analysis		
6	Monitoring and Analytics	Operations / Monitoring	Implement monitoring for virtual machines and workloads and mechanism to share the findings with UIIC periodically		
7	Monitoring and Analytics	Operations / Monitoring	Provide configuration options, aligned with best practices, for monitoring tools to gather performance and health status of resources, including on-premises applications.		
8	Monitoring and Analytics	Operations / Monitoring	Offer options for centralized logging and analysis, aligned with best practices, including capabilities for on-premises applications		
9	Monitoring and Analytics	Operations / Monitoring	Implement alerts and notifications for critical events, resource utilization, and anomalies based on machine learning.		
10	Monitoring and Analytics	Operations / Monitoring	Describe the process for storing, securing, and analyzing logs in accordance with the UIIC's requirements.		
11	FinOps	Cost Monitoring	Outline a complete costing model, cloud service provider charges, monitoring capabilities, customer access to current and historical cost information, alerting functionality, and measures for cost optimization.		
12	FinOps	Cost Monitoring	Ability to implement tools and practices for tracking and optimizing cloud spending.		
13	FinOps	Cost Monitoring	Ability to implement strong measures and methods to contain cloud costs, including the use of cost management tools and budgeting practices.		
14	FinOps	Cost Monitoring	Ability to implement a resource tagging strategy to effectively track and manage costs.⍰		
15	FinOps	Cost Monitoring	Ability to provide options for cost management tools to optimize cloud spending and resource utilization.⍰		
16	FinOps	Cost Monitoring	Ability to establish automated cost alerts to monitor and contain consumption.⍰		
17	FinOps	Cost Optimization	The bidder should propose a pricing model that accommodates scalability needs and ensures cost-effectiveness.		
18	FinOps	Cost Optimization	Bidder to ensure the cost of running the operations in cloud is optimized at all the times		
19	FinOps	Cost Optimization	Capability to deliver FinOps support, including recommendations and cost control measures.		
20	FinOps	Cost Optimization	Vendor must regularly review and optimize cloud resource usage for cost efficiency and performance.		
21	FinOps	Budgeting and Forecasting	Capability to create accurate budgets and forecasts based on usage patterns.		
22	FinOps	Resource Optimization	Ability to analyze resource utilization and identify opportunities for optimization.		
23	FinOps	Billing Transparency	Capability to provide clear visibility into cloud costs and usage.		
24	FinOps	Financial Accountability	Ability to establish accountability for cloud spending by assigning budgets.		
25	SysOps	Infrastructure Management	Ability to automate the deployment, monitoring, and management of cloud infrastructure.		
26	SysOps	Incident Response	Capability to implement robust incident response protocols.		
27	SysOps	Performance Monitoring	Ability to utilize monitoring tools to track system performance and resource utilization.		
28	SysOps	Configuration Management	Ability to manage and enforce configuration standards across cloud resources.		
29	SysOps	Operations / Optimization	Describe services that **optimize cloud capacity usage** for reliable and cost-efficient operations, including capacity planning and demand management.		
H. Availability, Backup & Recovery					
1	Operations / Resilience	High Availability	Design and implement high availability architectures to minimize downtime		
2	Operations / Resilience	Backup and Recovery	Describe **backup services** for protecting UIIC data, including backup granularity and recovery options.		
3	Operations / Resilience	Cloud Backup	Implement Cloud Backup for App Services, databases, and storage accounts		
4	Operations / Resilience	Disaster Recovery	Define **disaster recovery services**, self-service capabilities, and the RPO and RTO service levels provided by cloud service providers.		
5	Operations / Resilience	Disaster Recovery	Ability to test recovery plans to ensure they meet organizational Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements.⍰		
6	Operations / Resilience	Disaster Recovery	Ability to create and test procedures during disaster recovery (DR) events, including plans to fail workloads to the cloud and recover workloads from the cloud to on-premises data centers.		
7	Operations / Resilience	Disaster Recovery	**Develop and test disaster recovery plans** to ensure data integrity and facilitate quick recovery		
8	Operations / Resilience	Disaster Recovery	Implement **disaster recovery strategies** with cross-region replication to ensure data availability		
9	Operations / Resilience	Disaster Recovery	Ability to **utilize multi-region customer-managed CMKs** to enhance disaster recovery and cross-region replication, ensuring consistent key management and compliance across primary and DR regions while improving availability and aligning with enterprise-grade security standards.		
10	Operations / Resilience	Backup and Recovery	Capability to establish automated backup processes and disaster recovery plans.		
I. Governance					
1	Governance	Governance/Account Management Servi	Functionalities to quickly establish and manage a secure, multi-account cloud environment in accordance with best practices		
2	Governance	Governance/Account Management Servi	**Landing Zone Setup ->** Ability to automate the setup of a secure baseline cloud environment with centralized governance.		
3	Governance	Governance/Account Management Servi	**Account Vending ->** Provision new Cloud accounts efficiently using Account Factory for streamlined account vending.		
4	Governance	Governance/Account Management Servi	**Guardrails ->** Ability to enforce security and compliance through predefined policies based on cloud Config rules and Service Control Policies (SCPs) with Guardrails		
5	Governance	Governance/Account Management Servi	**Single Pane of Governance ->** Provide a centralized dashboard for viewing compliance and activity across accounts, ensuring a single pane of governance.		
6	Governance	Governance/Account Management Servi	**Blueprints ->** Ability to utilize standard templates for account structure, logging, and security baselines through applicable tools/technologies, promoting consistency and best practices.		
7	Governance	Security, Auditing, and Logging	Ability to house essential accounts that provide centralized security, auditing, and logging for the entire cloud environment.		
8	Governance	Security, Auditing, and Logging	**Centralized Logging:** Ability to maintain a centralized **log archive account** where logs from all accounts are stored securely, ensuring that logs cannot be tampered with locally.		
9	Governance	Security, Auditing, and Logging	**Security and Audit:** Ability to utilize a dedicated **audit account** for security teams to monitor activity, run security tools, and inspect compliance without being in the same account as the workload.		
10	Governance	Security, Auditing, and Logging	**Isolation from Workloads:** Ability to keep accounts separate from development, testing, and production environments to minimize the blast radius in the event of a compromise.		
11	Governance	Security, Auditing, and Logging	**Compliance and Forensics:** Ability to retain logs and audit trails outside of workload accounts to meet compliance requirements (e.g., PCI-DSS, HIPAA, ISO 27001), ensuring logs are preserved even if a workload account is breached.		

12	Governance	Security, Auditing, and Logging	**Unmodifiable Guardrails:** Ability to implement mandatory guardrails that cannot be disabled, ensuring a baseline level of security and governance across the cloud environment.		
13	Governance	Security, Auditing, and Logging	Log Archive Account: Ability to store centralized logs, including CloudTrail logs, configuration snapshots, and VPC flow logs from all accounts.		
14	Governance	Security, Auditing, and Logging	Audit Account: Ability to provide security teams and tools with read-only visibility into all other accounts for monitoring and auditing purposes		
15	Governance	Security, Auditing, and Logging	Security Tooling Account: Ability to host threat detection tools and security solutions, such as security monitoring platforms and third-party SIEM solutions, to enhance overall security posture.		
16	Governance	Security, Auditing, and Logging	Establish baseline policies that are aligned with best practices for governance and resource management within the cloud environment		
17	Governance	Security, Auditing, and Logging	Ability to support UIIC authorized audit personnel to review audit logs and monitoring data at any time within the CSP's data center		
18	Governance	Security, Auditing, and Logging	CSP should have legal frameworks and compliance for data residency, services residency including environments, data handling, security breach reporting and electronic data records		
J. Cloud Security					
1	Security and Compliance	Network Security Group	Incorporate best practices for network security groups to enhance security and control network traffic		
2	Security and Compliance	Vulnerability Management	Ability to incorporate best practices for vulnerability assessment and patch management processes.		
3	Security and Compliance	Vulnerability Management	The CSP should have the ability to offer Automated Sensitive/PII data discovery and classification, vulnerability management, threat detection, and prevention.		
4	SecOps	Vulnerability Management	Ability to conduct regular vulnerability assessments and penetration testing.		
5	Security and Compliance	Security and Logging Practices⍰	Provide options that support security and logging best practices.		
6	Security and Compliance	Securing the Cloud Environment	Provide details of services for protecting the cloud environment from security threats, including comprehensive IT Security Services offered by CSPs and how the UIIC can utilize those services.		
7	Security and Compliance	Securing the Cloud Environment	Implement best practices for security monitoring and threat detection using security tools, including security centers or third-party options as selected by UIIC.		
8	Security and Compliance	Securing the Cloud Environment	Ensure compliance with the Voluntary Product Accessibility Template (VPAT) by conducting accessibility assessments and providing documentation		
9	Security	Foundation / Governance	Implement **RBAC in the landing zone** to manage user permissions and access rights based on defined roles, ensuring secure and efficient resource management across the cloud environment		
10	Security	Foundation / Governance	Implement Identity and Access Management (IDAM) policies for internal UIIC employees by enforcing Multi-Factor Authentication (MFA) and utilizing Single Sign-On (SSO) for enhanced security.		
11	Security	Foundation / Governance	Implement Identity and Access Management (IDAM) policies for non UIIC / external employees by enforcing Multi-Factor Authentication (MFA) and utilizing a form-based approach with username and password for secure access.		
12	Security	Foundation / Governance	Design a domain controller within the cloud environment that adheres to best practice configurations.		
13	Security	Foundation / Governance	Implement identity protection measures following best practices to enhance security.		
14	Security	Foundation / Governance	Establish best practice implementation of conditional access policies within the cloud environment to manage user access effectively		
15	Security	Foundation / Governance	Integrate **Cloud KMS (Key Management Service)** to enforce encryption-at-rest and ensure regulatory compliance for sensitive data across services like Amazon S3, CloudWatch Logs, and Systems Manager etc.		
16	Security	Foundation / Governance	Provide encryption options for data at rest and in transit, with the approach to be selected by the UIIC.⍰		
17	Security	Foundation / Governance	Support UIIC in maintaining its own encryption keys using a key management solution.		
18	Security	Foundation / Governance	Provide **centralized control over cryptographic keys**, implement IAM-based permissions on key usage, and manage key rotation and audit logs via CloudTrail.		
19	Security	Foundation / Governance	Implement robust security measures, including **firewalls**, **encryption**, and **access controls**		
20	Security	Key Vault	Deploy and configure **Cloud Key Vault** for the secure storage of keys, certificates, and secrets		
21	Security	Cloud Firewall	Deploy **Cloud Firewall** to manage inbound and outbound traffic		
22	Security	Cloud Firewall	Define **Network Security Groups (NSG)** and establish firewall policies		
23	Security	Security Services⍰	Ability to offer dedicated cryptographic functions, Cloud security posture management, Secrets and configuration manager, secured VPN, etc., from the India region.		
24	Security	Data Protection Services⍰	Availability of service having the ability to automatically discover, classify, and protect sensitive data including PII data and IP, with the ability to continuously learn and adapt to evolving data patterns through customizable detection criteria and serverless autoscaling architecture.		
25	SecOps	Security Monitoring	Ability to implement continuous security monitoring to detect threats.		
26	SecOps	Access Control	Capability to enforce strict access controls and identity management practices.		
27	SecOps	Access Management	Ability to offer automated Permission and Access Risk Analysis with the ability to assess resource-level permissions across subscriptions or tenants and provide resource-specific continuous automated risk detection, policy validation, and simulation, tightly integrated with other cloud-native security insight services to provide enterprise-wide governance and compliance visibility.		
28	SecOps	Compliance Management	Ability to ensure adherence to regulatory and industry standards.		
29	SecOps	Incident Management	Capability to establish incident response plans for security breaches.		
K. Miscellaneous					
1	Operations / Support	Incident Management	Implement a **robust incident management process** for the quick detection and resolution of issues		
2	Operations / Support	User Support and Training	Provide **support and training to users** for effective utilization of cloud resources		
3	Operations / Support	User Support and Training	Develop **documentation** and **conduct training sessions** for users		
4	Operations / Support	Support in Onboarding New Application (	The bidder is required to provide support for future applications, which should be backed by a rate card for cloud specialist roles		
5	Operations / Support	Support for Cloud Infrastructure	The vendor must clearly state the proposed support service tier (e.g., Basic, Standard, Premium, Platinum, Enterprise) and detail what each tier includes (response times, escalation paths, dedicated account managers, etc.).		
6	Operations / Support	Support for Cloud Infrastructure	The vendor must act as the primary liaison with the CSP for all cloud infrastructure -related issues, including incident resolution, service requests, and escalations.		
7	Operations / Support	Support for Cloud Infrastructure	Provide a documented escalation matrix with CSP contacts and timelines.		
8	Operations / Support	Support for Cloud Infrastructure	Vendor must ensure timely upgrade of cloud services including service packs, patches, version upgrades of software and components in coordination with CSP		
9	Operations / Support	Support for Cloud Infrastructure	Vendor must handle all cloud-related service requests (e.g., provisioning VMs, storage, networking) via ticketing tool		
10	Operations / Support	Support for Cloud Infrastructure	Vendor must maintain up-to-date documentation of cloud architecture, configurations, and support processes.		

D. Technology Stack

Sr No.	Technology Area	Technology Component/Requirement as per inputs from Bidder. (Any deviation to be with justification and how it will improve the outcome.)	Bidder Proposed Technology/Tools (Mention Tools/Components Provisioned with Version where applicable.) Mention about Licensing, OEM, nature (if applicable) and the duration and quantity provisioned	Bidder Remarks, Justification in case there is any deviation from the proposed technology/tools etc.
1	**Client Side**	Modern JavaScript Framework - React	<Bidder to propose and include in the solution>	
2	**Framework (Server Side)**	Spring Boot, JPA: Spring Data with Hibernate	<Bidder to propose and include in the solution>	
3	**Backend OS**	Redhat Enterprise Linux or equivalent enterprise grade OS	<Bidder to propose and include in the solution>	
4	**Containerization / Management**	Kubernetes #	<Bidder to propose and include in the solution>	
5	**API Manager**	Kong #	<Bidder to propose and include in the solution>	
6	**ESB**	Apache Camel #	<Bidder to propose and include in the solution>	
7	**ODS**	PostgreSQL #	<Bidder to propose and include in the solution>	
8	**Development**	Version control with git CI/CD	<Bidder to propose and include in the solution>	
9	**Web/App**	Nginx, Tomcat, Docker containers	<Bidder to propose and include in the solution>	
10	**Service Mesh**	Istio #	<Bidder to propose and include in the solution>	
11	**Identity & Access Management**	Open-Source Enterprise Grade (KeyCloak) Protocol Supported: OpenID Connect, OAuth 2.0, and SAML 2.0 Integration: LDAP /AD Support Single Sign-On and Single	<Bidder to propose and include in the solution>	
12	**Log Management and Observability**	ELK stack (Elasticsearch, Logstash, Kibana) Open-source monitoring tools such as Grafana and Prometheus or Elastic APM	<Bidder to propose and include in the solution>	
13	**Document Store**	NoSQL DBs – MongoDB #	<Bidder to propose and include in the solution>	
14	**Messaging**	Kafka	<Bidder to propose and include in the solution>	
15	**Cache**	Open Source in Memory Cache - Redis	<Bidder to propose and include in the solution>	
16	**Project Management / Change Management**	Jira / Confluence	<Bidder to propose and include in the solution>	
17	**Secure Code Review / Analyzer**	SonarQube	<Bidder to propose and include in the solution>	
18	**SMS Gateway**	UIIC Provided API Based Integration (Two Service Providers)	<Bidder to propose and include in the solution>	
19	**Email Gateway**	UIIC Provided API Based Integration (Two Service Providers)	<Bidder to propose and include in the solution>	
20	**WhatsApp**	Integrate with UIIC WhatsApp Enterprise/Business account	<Bidder to propose and include in the solution>	
21	**Security**	OWASP and SANS Verified Anti Hack Preventions	<Bidder to propose and include in the solution>	
22	**Rule Engine / Rule Management**	Drools	<Bidder to propose and include in the solution>	
23	**IDE**	Spring Tool Suite	<Bidder to propose and include in the solution>	
24	**Benchmarking**	JMeter	<Bidder to propose and include in the solution>	

# Components should be provided with "Enterprise Grade Support" as part of the solution to eliminate the need for community support and ensure timely resolution/support during production issues.

E. Additional Requirements

Sr No.	Additional Technology Area	Technology Component/Requirement as per inputs from Bidder	Bidder Justification and Remarks to support inclusion of this component in the proposed solution
1	Security	<Bidder to propose and include in the solution>	
2	Key Management	<Bidder to propose and include in the solution>	
3	Networking	<Bidder to propose and include in the solution>	
4	Storage	<Bidder to propose and include in the solution>	
5	*<Bidder to add as applicable>*	<Bidder to propose and include in the solution>	

F. DevOps Tool Chain

Sr No.	Technology Area	Technology Component/Requirement as per inputs from Bidder.	Bidder Response	Bidder Remarks, if any
1	Source Control Repository	Git		
2	CI/CD	Jenkins, Maven, Ansible Playbook		
3	Agile Process/Agile software development	Jira and Confluence		
4	Test Automation	Selenium		
5	Secure Code Review/Analyzer/SAST/QA	Junit, BrowserStack, SonarQube		
6	Web Application Security / DAST	OWASP ZAP		