Request for Proposal

Implementation & Maintenance of Unified Digital Interface for PMSBY/PMJJBY schemes

Issued By:

General Insurance Council

Life Insurance Council

Indian Banks Association

Contents

1 Introduction:

1.1 About the project:

The Government of India announced social security schemes Pradhan Mantri Jeevan Jyoti Bima Yojana (PMJJBY) and Pradhan Mantri Suraksha Bima Yojana (PMSBY) in the year 2015. These schemes are aimed at creating social security system for all Indians especially the poor and underprivileged at an affordable premium.

These schemes are being offered by insurers in tie-ups with Banks and Post-offices and are annual in nature. It is proposed to create a Unified Digital Interface (UDI) for ensuring seamless end to end connectivity between various stakeholders. This IT platform could connect insurance companies and their partner banks to undertake enrolments and promote speedy and seamless claims settlement and MIS generation in respect of PMJJBY and PMSBY. The platform is being jointly created and operated by the General Insurance (GI) Council, Life Insurance (LI) Council and Indian Banks' Association (IBA) , hereafter referred to as Contracting Party.

1.2 About the engagement:

Unified Digital Interface application provides a set of interfaces linking and integrating various stakeholders e.g., insurance companies and their partner banks for transfer and exchange of data. This application closely mirrors the objectives of the intended UDI platform and is required to be enhanced and managed as per the final scope mentioned in this RFP document. The vendor would be required to develop master data repository and to host it with the application to act as a common data pool and analytics platform apart from managing the workflows including enrollment, issuance of COI, claims and grievance management and tracking for the insuring segment and concerned stakeholders. This may also entail minor enhancement/ modifications in the existing framework to achieve the above objectives. Once deployed the vendor shall be required to migrate historical data available with insurance companies and their partner banks.

1.3 Stakeholders and users of Platform

a) Public/ Private sector banks including Regional Rural Banks (RRBs) and cooperative banks
b) Life Insurers implementing PMJJBY
c) General Insurance companies implementing PMSBY
d) Government of India - Department of Financial Services
e) e-SHRAM portal maintained by Ministry of Labour & Employment (MoLE) and other similar platforms
f) General Insurance Council
g) Life Insurance Council
h) Indian Banks' Association
i) Insurance Regulatory and Development Authority of India (IRDAI)

j) Reserve Bank of India (RBI), National Bank for Agriculture and Rural Development (NABARD) and other stakeholders

2 Eligibility Criteria

The Bidder should be an approved/ promoted repository of the governing bodies of the entities involved in this project, and thus be approved by IRDAI or RBI or SEBI or NABARD.

S.No.	Bidder Eligibility Criteria	Supporting Documents
1	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in existence in India for more than five (05) years as on bid submission date.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2	The Bidder should have had a minimum average turnover of INR 50 crore in each of the last three financial years (2018-2019, 2019-2020 and 2020-2021).	Copy of Audited Financial statements for the financial years (2018-2019, 2019-2020 and 2020-2021) And CA Certificate
3	The Bidder should have a positive Net-Worth in each of the last three financial years (2018-2019, 2019-2020 and 2020-2021).	Copy of Audited Financial statements for the financial years (2018-2019, 2019-2020 and 2020-2021) And CA Certificate
4	The bidder should not be debarred / black-listed by any Government or PSU enterprise in India as on date of the submission of RFP.	Undertaking to this effect to be submitted on Company Letterhead
5	The bidder should be an OEM or a certified or authorized agent/ reseller/ partner of the solution offered Product	Manufacturer's Authorization Form
6	The bidder should be a cloud service provider or a certified partner of cloud service provider or run their own data center/ repository. In case of a Bidder, who is proposing to use a Cloud service, bidder should have an agreement to host service on cloud and back-to-back support agreement with the cloud service provider.	Manufacturer's Authorization Form
7	The Bidder should be an approved/ promoted repository.	Indication on website or letter of authorisation to store financial data

S.No.	Bidder Eligibility Criteria	Supporting Documents
8	Bidder should have its own Support center or provide for support for Telephonic and Remote Assistance Services in Delhi, Mumbai / Navi Mumbai	Self-Declaration along with the details of the support centers in Delhi, Mumbai / Navi Mumbai.

2.1 Compliance with Prescribed Standards

The proposed solution has to be based on and compliant with the latest industry standards wherever applicable. There are many standards that are indicated throughout this RFP as well as summarized below. The list below is just for reference and is not to be treated as exhaustive.

S. No.	Component/Application/System	Prescribed Standard
1.	Workflow Design	WFMC/BPM Standard
2.	Portal Development	W3C Specification
3.	Information Access / Transfer Protocols	SOAP, REST, HTTP/HTTPS
4.	Interoperability	Web Services, Open Standard
5.	Document Encryption	PKCS specification
6.	Information Security	ISO 27001 certified system
7.	Operational Integrity & Security Maintenance	ISO 27002 certified system
8.	Operations	ISO 9001 certified
9.	IT Infrastructure Maintenance	ITIL/EITM specification
10.	Service Maintenance	ISO 20000 specifications or latest
11.	Project Documentation	IEEE/ISO specifications for documentation

Table 1: Compliance with Industry Standards

A declaration to that effect in the form of undertaking needs to be submitted by the bidder along with the technical bids.

3 Technical bid parts:

The bidders should understand the requirements in detail and propose best solutions in hardware/software that would fit the required task in terms of choice of database, technology platform, operating systems, cloud systems and associated hardware, etc., that are inter-operable, optimally priced and provide for easy maintenance and upgradation.

The solution should be robust, scalable, frugal, inter-operable, federated and non-monolithic.

A detailed plan would be submitted with the technical bid and each bidder would be given an opportunity to present the suitability and rationale behind the components chosen and the overall process flow proposed.

The proposal involves the following parts:

a) Overall architecture and systems solution including Hardware/Software
b) Enhance the existing processes and workflows
c) Proposed technology solutions
d) Cloud services & management
e) Networking services & management
f) Setup of database and tools
g) Migration of data
h) Handling of privacy and confidentiality norms
i) Security features
j) Creation of interfaces and support
k) Testing
l) Documentation
m) Support for the project
n) Audit
o) Disaster recovery

3.1 Technical Framework of existing setup

The existing application Unified Digital Interface has been using the following technical specification

a. Net framework 4.5 +
b. UI/UX developed on web forms
c. Rest based API
d. Database -Oracle DB 18C
e. Browser compatibility - Google Chrome
f. Batch processing tools
g. IIS 10 server
h. Windows 16 enterprise edition
i. API for SMS
j. Mail server for sending communication on email

3.2 Technical Framework for proposed common platform

The development of the repository and the new interfaces should be in sync with the proposed UDI application.

S.no	Description	Recommended Technology Stack

1	Platform Installation & Configurations	1. Frontend to be in React JS and latest Java script Library like TailwindCSS and Material UI 2. Backend services to be in latest stable version of Spring Boot **3. DB to be any open source or any RDBMS or combination of both however there has to be a proper OEM support and road map of the DB which needs to be submit with technical proposal** 4. Provision to support No SQL and Big data requirements (support for MongoDB / Cassandra 5. Microservices orchestrated via Kubernetes 6. Access any data flexibly and easily: Access data in multiple formats (including CSV, Excel, and JSON), multiple sources (including object storage, Oracle Database, MongoDB, PostgreSQL, and Hadoop), and multiple locations (on premises, Cloud, and other clouds). 7. Design should support Auto scaling (Up & Down) of compute based on metrics (CPU & Memory) & time/schedule based to align with business demand like month end peak, quarterly & annual peak. 8. Support all current and future technology like Analytics, Blockchain or future technology On-Demand basis. 9. Integration platform should be implemented using SOA and must support ESB
2	Search Capabilities	Search capabilities on top of database Search capabilities using Elastic (ELK) Stack -Powerful search for documents and results living in websites, applications, and workplaces.
3	Devops	1. (CI/CD -Continuous Integration/Continuous Delivery) tools like Jenkins etc., 2. version control through Git / Github, 3. Log data analysis from any source and create helpful visualizations for data analysis through storage with Elastic search, processing and data collection with Logstash and visualization with Kibana (ELK Stack), 4. Implementation of microservices deployment and orchestration tools like Kubernetes/Docker Swarm

4	Security	1. Compliance of ISNP/ISMS guidelines 2. Project to use approved technology and meets all information security policies 3. Threat prevention, detection, and response with SIEM and endpoint security 4. VAPT/WASA 5. Encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm. 6. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later. (valid certificate and expiry management of certificate) 7. Integration with SIEM for log collection. 8. Integration with key manager for storing the keys 9. Static/dynamic code analysis following secure coding practices
5	Development	1. Full stack development is to be done using opensource enterprise Java frameworks like Spring Boot for backend and Frontend to be in opensource frameworks like React JS and latest Java script Library like Tailwind etc. 2. Develop RESTFUL API's FOR data interchange and workflow integration. Add on to the Unified Digital Interface supported APIs. 3. Detailed documentation of API along with versioning 4. Develop middle ware logic and rules 5. Develop the database logic 6. Ability to integrate with existing systems and 3rd Party (IIB, Aadhar, NSDL, Payment Gateways), Communication (SMS gateway, SMTP gateway), Google Analytics, etc. 7. API Gateway implementation as mentioned in the RFP 8. The website to be compatible with the upcoming potential user front end, by adapting to Headless Architecture (Decoupled architecture) by providing data to be rendered in json/XML format and delivers it in the raw form to the front-end wherever required 9. Cloud Native MicroServices Architecture Implementation 10. Provisioning of enterprise content management 11. Distributed Cache implementation 12. ETL implementation for data synchronization (De-Dupe check using parameters like name, father's name, age, dob etc. on Client Master table) 13. Base one-time data to be migrated from existing silos

		14. Master Data Repository (local data mart) to support Analytics and existing MIS templates 15. Application Performance Management tool implementation as mentioned in the RFP 16. DevOps & DevSec Ops implementation 17. BILINGUAL version to be there These are available with Unified Digital Interface App and may need to be enhanced and supported for the duration of the project 18. Online Claims registration 19. Quote Generation to Policy issuance 20. New business, endorsement, renewal, claim, servicing 21. Content management Solution 22. Workflow implementation 23. For Grievance Redressal existing system integration to be done which is provided by IRDA as well as a new Grievance Redressal system needs to implement which will be an enterprise system for UDI. 24. BILINGUAL version to be there 25. Role based logins and dashboards for all stakeholders including Agent/intermediary role and Hierarchy Management using front end form. 26. All kinds of SOP preparation like key management, BCP documents, log management etc.
6	Database	1. Bidder needs to customize the database as per the requirement finalized during SRS phase 2. Application and database to be hosted on the virtual private cloud
7	Monitoring Tools	1. Cloud based API tool 2. Cloud based APM tool
8	Disaster Recovery	1. Cloud based ADR tool / DRaaS 2. DNS FAIL OVER / GSLB
9	DevSecOps	DevSecOps through Code Analysis, Automated Testing, Change Management, Compliance Monitoring, Threat Investigation, Personnel Training for security integration across all stages of the software development process chain, addressing security concerns at the very start of every stage has to be ensured
10	Analytics on Cloud	Vendor/SI/MSP/CSP to enable accessing data sources across on-premises and the cloud infrastructure, model -that data and provide business users with a simplified view of their data to

		enable interactive self-service BI and data discovery using their preferred data visualization tool

The above-mentioned tools/software are indicative only. Any solution that meets the requirement and is cost effective can be proposed and implemented as per approval from contracting parties.

4 Scope of Work

The scope of work under this project is two-fold.

The software for the UDI platform has been created and tested. The software takes care of the basic functional requirements of the project. The application will need to be maintained and enhanced as needed under this project.

The hardware and the infrastructure for hosting the application and creating and managing the data repository would form the crux of the project. The entire structure would need to be designed and managed for running the application, over 5 years of operation.

4.1 Overview of Activities

1. Design, Supply, Implement, Hosting and Operation of a common data repository and migration of historical data (more than 35 crores transactional datasets at the last count) from existing repositories of various Govt. led web based platforms, Banks and Insurance companies as per the common data standards after proper reconciliation and de-duplication in the target common data repository
    i. Primary & DR sites management responsibility either through self or cloud service provider (CSP) with 4 hours RTO and 1 hour RPO maximum.
    ii. Architecture design (multi-tier) and adequate infra sizing based on the current transaction volume, concurrency, peak loads and future growth to provide high performance of <150ms
    iii. High uptime & availability of 99.9999%
    iv. Hosting in India

2. Hosting of existing “Unified Digital Interface” application- To setup and manage the hosting of the application and data Infrastructure in the new hosting environment to be provided, designed, tuned and managed by the bidder

3. Maintenance of the existing Unified Digital Interface framework and its preexisting modules such as
    a) Registration, login, user management using identity and access management tool
    b) Enrolments, entry of enrolments by the registered banks,
    c) Capturing of Risk details
    d) Collection and transfer of premium
    e) Issuance of certificates of insurance, via SMS/email
    f) Generation of renewal information

g) Claims handling. capture of the claim data, information to insurer and the final status of the claim.
h) Grievance Management – entry of complaints and grievances, notifications to banks/ insurers and status of handling
i) Reports/MIS and Analytics
j) Identity Management
k) Notifications and reminders on email and SMS

Enhancements as necessary to the above modules, as per the testing and migration and usage of the system during the UAT phase.

4. Segregation of environments and user roles e.g. Development, SIT, UAT, Pre-Production and production environments.

5. Information security:
    a. As per regulatory norms of the land.
    b. Implementation of Firewalls (perimeter and WAF), Antivirus, SSL etc
    c. Patching and upgrade of OS/DB/Application and Application Infrastructure components
    d. Data backup and restoration as per standard policy
    e. Conducting Information Security assessment such as VA/PT, Source Code review etc. with regular audits from Cert-in certified vendor.
    f. DR drills every half yearly
    g. Implementation of Aadhar data vault as per UIDAI instructions

6. Enhancement and Capacity management for 3 years of operation:
    a. End-to-end Change Request Management with proper audit trails
    b. Governance model for monitoring on-time delivery
    c. Enhancement and Capacity Management of platform Infrastructure to maintain performance and SLA.
    d. Project and ticket tracking tools for raising and tracking requests.
    e. Request and Incidence management

7. Migration of data from the various stakeholders of the last 5 years of operation.
   Support the applications and build in the enhancements as regards advanced de-duplication and interfaces as also support the integration of the Unified Digital Interface app with the banks /insurers.

8. Helpdesk with adequate staffing
    a. Handling all issues faced in production environment with adequate ticket tracking solution in place (e.g. JIRA).
    b. L1, L2 & L3 levels for request and incidence management

9. Training & Handholding
    a. TTT with adequate/extensive online training modules
    b. Hand-holding during launch of the module.

c. Handholding the stakeholders who would interact with the platform is also part of the scope.

To enable the development of all modules, yet keeping in line with the timelines prescribed, the project is envisaged in various parts as has been explained further.

5 Hardware

Bidder is required to size, supply, design, commission and maintain hardware, OS, DB as well as all software required for the proposed applications that should be as per the contract duration mentioned in RFP document for all environments, i.e. DC, DR and Non-Production (Test, Development, UAT, pre-prod& Training).

Bidder needs to provide all the details of each components (server, storage, space, middleware, SAN Switch, Tor switch, or any other component required as part of the solution) like make, model, configuration, architecture, etc. Bidder should consider high availability at all three layers for UDI web-based platform and app. Web-layer and Application layer should be load balanced in Active- Active at DC and DRC and database layer can be proposed in active-passive.

The hardware details must include:

- Server and Storage (usable capacity and RAID) requirement
- Production Environment (Web, Application, Database, Middleware etc.) at DC and DRC
- All Non-prod (Test &Development, UAT, Training and Pre-prod) Environment at DC

The Design, of the hardware should be such that at any point in time during the contract period, the **average CPU utilization should not exceed 70% at the primary data center and Disaster Recovery Center**. Bidder is required to submit the sizing adequacy.

Bidder will have to deploy hardware resources at DC and DR as per the project plan on the proposed cloud. Hardware technology proposed by the bidder should be based on the latest offerings by the respective OEMs. The hardware should be of enterprise class, best of breed, tested and stable release of OEM.

Vertical and horizontal scalability should be two important requirements for these cloud deployment and application development.

Cloud storage should also support storage efficiency features like thin provisioning, deduplication and compression to reduce the primary storage capacity requirement.

Cloud Storage should support backup on low-cost object storage. All the storage efficiency benefits should be available on object storage also to reduce secondary storage requirement.

Cloud Storage should have the flexibility to move data from one public cloud to other Public clouds seamlessly.

Bidder should arrive at the sizing independently keeping growth roadmap in consideration. Also, during the contract period, growth of the UDI should be considered and thus, the hardware proposed should have enough CPUs, memory and storage available to accommodate the predicted sizing required.

DB audit trail should be enabled across all environments and bidder is required to size the hardware accordingly.

As per the architecture there are 5 copies of databases required at DC. Prod, test & Dev, Training, UAT & Pre-prod with a performance neutral volume clones for each of the workloads and a full volume copy. These copies shall have incremental updates. Taking of backup for the onsite tools proposed in the RFP will the responsibility of the bidder and bidder needs to factor necessary equipment and cost for the same.

Bidder can consider logical separation/virtualization for production and non-production environment at compute and storage level for respective environments.

The bidder should note that the production and non-production environment should be physically separate with respect to compute.

The Pre-Prod servers sized should be minimum 25% of the size of the production as per the fifth-year sizing however the database size will be similar to production database size.

The Test, Development, UAT& Training servers should be minimum of 10% respectively of the size of the production as per the fifth-year sizing however, the database size will be similar to production database size.

The bidder can propose the latest version of industry leading RDBMS software.

Bidder is required to perform the following activities other than the ones called out as part of responsibility matrix below:

1. Installation/ Creation/ Re-Installation of databases with suitable hardening procedures as per Bank's policy.
2. Fine tune and resolve performance issues through performance tuning and optimizations.
3. Provide the required operational support to monitor the proposed applications database environments.
4. Refer to the successful backup and restoration of the database instances as defined by contracting party.
5. Management of the granting, removal, monitoring and editing of access rights allocated to the database and application environments based on the direction and approval of the contracting party.

6. Processes to perform database upgrades, performance tuning and repairing a database (if required).

7. Create, implement and validate database recovery solutions. Support during DR testing and during actual DR situations

5.1 Network and Network management

All maintenance and management of the various component will be handled by the vendor. Some of the activities include:

- Configuration of multiple networks
- Creation of domains isolated for access by different types of stakeholders
- Firewalls for general access
- Security mechanisms to be implemented at network level and server level
- Rules and access control for different types of users – server level and database level
- Key vaults or similar solution if and as needed
- Managing the active directory, including LDAP if necessary
- Management of network traffic
- Regular audits and maintenance through SIEM tools (Security information and event management) etc.

While it is assumed that the cloud end configuration would be standardised, monitoring of the same and needed interventions and end-point connectivity issues to be handled by the vendor.

5.2 Cloud and Cloud management

The vendor can suggest the best cloud system for this purpose. The options could range from using the commercial clouds such as AWS, Azure, Oracle Cloud, Sify Cloud etc. or suggest procuring and managing a private cloud. The reasons and rationale behind the suggestions to be clearly specified. Either way, the server management on cloud is the responsibility of the vendor.

The following to be taken note of while making the recommendation:

- Cloud to be based in India, preferably in or near Mumbai
- The DR of the cloud to also be based within India, in a different seismic zone
- Backup of the data to be planned on the cloud with regular backup routine recommended to be specified
- Expertise on working with multiple cloud instances and inter-operability is a must
- Expertise with deploying and maintaining large scale data repository on cloud
- Management of the cloud instance and maintenance of the cloud including managing of any new DR/cloud instance that may be added necessitated by the data and

applications, during the tenancy of the project timelines, is within the scope of the project.

- Adhering to ISO 27017 and IRDAI cloud security guidelines
- For all cloud components, keeping the elastic nature of the cloud, the vendor has to provide for a unit price for compute, storage and other components. This will ensure that a minimum set of cloud infrastructure will be paid monthly and items like storage will be increased monthly to ensure optimum costs.

5.3 Database management

The scope of the database management services includes all data and database management of in scope applications (Oracle, SQL, etc.) activities on the production, non-production and disaster recovery environment that will be included as part of this service. The expected database management services can be further defined by the following high-level service requirements:

Domain services	Description
Build and Installation	Definition/Installation/Creation of databases with suitable hardening procedures as per contracting party.
Database Performance Management	Fine tune and resolve performance issues through performance tuning and optimizations.
Database Capacity Management	Estimate & recommend database requirements based on performance and Business projections
Monitoring and administration	Provides the required operational support to monitor UDI database environments.
Backup and restore	Refers to the successful backup and restoration of the database instances as defined by contracting party.
Access management	Management of the granting, removal, monitoring and editing of access rights allocated to the database environments.
Database adhoc support	Processes to perform database upgrades, performance tuning and repairing a database.
DC and DR testing	Create, Implement and validate database recovery solutions. Support during DR testing and during actual DR situations.

General

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines
2. Database and DBMS best practices will be a part of scope

Database Build and Installation

3. Defining the physical database design (log files, rollback segments, tablespaces, database descriptors, partitioned objects)
4. Installation of software and database creation [in consultation with the contracting party] - Oracle/ SQL etc. as per requirement of UDI
5. Create definitions of logical data structures, tables, views, indexes, program specification blocks, stored procedures & define their relationships
6. Hardening process document for fresh DB installation and perform hardening
7. Test and prepare database upgrades
8. Implement database upgrades into the production, non-production and DR environments
9. Publish Plan of Action (PoA) to be verified and validated by contracting party before implementation.

Database Performance Management

10. Track & co-ordinate database related incidents/problems till resolution
11. Conduct first level diagnosis for reported incidents & perform resolution
12. Analysis of incident/problem trends
13. Co-ordination & escalation to database vendors (L3) (logging ticket at vendor side as well internal tracking through service desk) and follow-up till resolution
14. Maintaining & monitoring the health & performance of databases (Primary and standby)
15. Monitor & analyze alerts & logs including -
    a. Trace files (including data block corruptions, enqueue resources, internal errors & I/O read-write failures)
    b. Database changes
    c. Background job status
    d. Operating system logs
    e. Space management
16. Monitoring the table space utilization, file system usage and all other events of O.S which may deter the performance of the database (primary as well as DR)
17. Analyzing/Troubleshooting Database Performance
18. Collection of statistics for databases
19. Optimizing database performance, performance tuning
20. Monitor physical DBMS for performance & capacity requirements, Databases and logs
21. Provide recommendations on DBMS design
22. Monitor the backup & report on backup logs
23. DDL, export & import related activities
24. Preparing monthly database related reports
25. Provide databases for MIS purpose on daily, monthly and on need basis

26. Periodic optimization of application databases through compression facilities and database tuning.
27. Provide reports on database currency and propose upgrade recommendations
28. The bidder is required to install & implement database diagnostics & fine-tuning packs based on UDI's requirements.

Database Capacity Management

29. Estimate & recommend database requirements based on received data from Database Performance team and Business projections (Annual/ As and when required)
30. Perform Database Space analysis and provide policies to maintain access sand performance
31. Review archive logs requirements
32. Customizations required at DB level

Database Monitoring and Administration

33. Setting data storage parameters for storage associated with the physical elements of the database
34. Encrypted passwords storage
35. Configuration of Databases
36. Managing, applying & verifying Database program patches & updates
37. Database Scripting
38. Coordinate all changes through the agreed upon change management process
39. Database recovery
40. Weekly database activities
41. Required logs maintenance as per Standards of the UDI
42. Recreation of Indexes
43. Responsible for maintaining DB inventory
44. Maintaining and performance tuning of UAT databases
45. Migration of Databases (Release Upgrade)
46. Resolving corruption (both Physical & Logical) issues at primary & standby databases
47. Designing &Implementation of logical & physical backups
48. Flash back up on daily basis
49. Using data guard and RAC for Oracle
50. Log shipping/Mirroring/Always On for SQL
51. Monitoring, management and implementation of High Availability (HA) viz. clustering/RAC etc.
52. Resolution of audit points and VA/PT reports
53. Management of tools
54. Monitor availability of the databases as a subset of monitoring overall service availability.
55. Providing solution services for database design, configuration and maintenance

56. Assist with incident and problem management related activities relating to the database environment (e.g. integration, interface, performance, configuration issues as part of the overall support service) including interaction with third party suppliers where necessary.
57. Archive of application specific data as requested.
58. Implementation and monitoring of database security.
59. Loading software components- Kernel patches, Release changes.
60. Documentation upkeep and records maintenance

Database Backup restore

61. Manage Database backup/ restore schedule, administration (RMAN Backup)/Scheduled Backups and others

Access management

62. Implementing & managing security rules & access authority as per required UDI's security policy, database Hardening etc.
63. Monitoring and management of logs for user access management of privileged users

Database adhoc support

64. Provide access to DBA resource for ad hoc work requests and change orders

Database Recovery

65. Create & implement database recovery solutions in consultation with contracting party
66. Evaluating current backup, recovery, & data replication procedures & providing recommendations for improving those procedures.

5.4 Server Management

The scope of the server Management services includes all RISC, EPIC, Wintel and Hyperconverged management activities on the production, non-production and disaster recovery environment that are part of this solution. The expected server/Hyperconverged Management services can be further defined by the following high-level service requirements:

Service	Description
Installation and configuration services	Refers to the appropriate installation and configuration of the server environment as per industry best practice as well as UDI's requirements.
Monitoring operations	Provides processes and procedures to monitor the server environment to ensure that the appropriate monitoring,

Operating system support	Provides for operating systems and related software configurations. The service also consists of ongoing processes to maintain supplier supported operating platforms for preventive software maintenance Services. This includes services such as: 1) Software configuration management 2) Software upgrades and patch management 3) Software release management 4) Software optimization, tuning and preventative maintenance
Hardware support	Provides the services and methodologies that will be used by the Bidder to support the UDI's server requirements. This service consists of the following components: 1) Hardware installation and configuration 2) Hardware environment support 3) Hardware preventative maintenance 4) Hardware refresh
Operating system security administration	Operating system security administration provides the processes to manage access to client assets at an operating system level. This security service provides the management of user logon ids and their access rights to system level resources, as well as maintaining server level security parameters and security product options. This section describes the various actions to be taken as part of the Security Administration Service, as well as what is needed on behalf of the client in order to provide these service levels.
System vulnerability management	Vulnerability management consists of preventive and detective services to identify vulnerabilities as they emerge; to prevent those vulnerabilities from affecting the in-scope systems; to detect when an in-scope system has been affected; and to cure those affected systems. Vulnerability management consists of both Vulnerability Alert management and Vulnerability Scanning processes. Vulnerability Alert management is the preventative process that collects known vulnerabilities and prioritizes vulnerabilities based on associated risk.

Operating system Security event logging	Operating system security event logging is a detective control that enables the recording of security events on system hosts based on present parameters. The administrative tool's logging function is enabled, and the security events are retained in a record for future review.
Performance and capacity management	Consist of the support processes to collect, monitor, and analyze system performance information, for processor usage, input/output (I/O) throughput activity, disk usage, and memory usage
Scheduling and monitoring	Scheduling and monitoring Process consist of those specific tasks associated with administering the automated scheduling system to provide the tools and processes necessary to support a scheduling and monitoring processing environment.
Failover management	Provides for the recovery of the critical workload on the server environments in the event of an outage of primary server and / or a disaster. The bidder is required to prepare documentation of a written recovery plan for the server environments

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines
2. Shifting of servers within the premises and reinstallation and configurations including cabling and asset labelling
3. Provide server configuration reports and configuration details to the UDI as requested
4. Implement configuration management processes and procedures.
5. Record and plan release of server upgrades and support its implementation
6. Maintain an audit trail of server configuration changes as resulting from release and change control processes.
7. The required software agents are to be installed, configured and monitored.
8. Provide guidance to the contracting party of industry best practice for the optimal configuration of the operating system environment
9. Produce and maintain installation and configuration diagrams of all installations
10. Actively manage and report on the availability of all servers
11. Perform server periodic checks, monitoring and performance tuning.
12. Communicate any service issues or implementation concerns with the UDI and appropriate support personnel and/or vendors
13. Monitor hardware and system software status, process status, and take necessary action based on detected problems or issues as provided in this schedule.
14. Provide problem escalation and interact as necessary with third party suppliers
15. Provide monitoring and troubleshooting for the server environment
16. Provide timely notification and escalation to on site personnel, if any

17. Bidders will ensure appropriate resources are on site to ensure service levels are achieved if recovery or corrective actions are required.
18. Propose tools for operations such as monitoring, deployment and configuration etc.
19. Ensure server access is secure and authorized
20. Management of logical access to the server environment in accordance with the UDI's requirement (including administrator \ root access)
21. Assist the UDI with application support requiring operating system changes or access
22. Evaluate the impact of new operating system upgrades or releases on existing applications and performance.
23. Install patches as and when these become available, per vendor instructions for security exposures and Operating System bug fixes deemed critical by the vendor.
24. Ensure the configuration of operating systems is in line with standards and policies as defined by the contracting party
25. Document and track all configuration management problems using the site change management process
26. Co-ordinate all changes through the site's change management process.
27. Configuration management for operating system release levels, patches and status.
28. Perform routine system operation functions and system console operations actions such as power on/off, system reboots, and start/stop/reset.
29. Apply preventive and corrective maintenance to all system level software (operating system and other non- application software).
30. Install and upgrade all system level software (the operating system and other non-application software).
31. Escalate hardware related malfunctions to the hardware supplier for resolution as provided in the vendor maintenance contract
32. Inventory information about hardware shipping and receiving, raised floor space requirements, equipment placement, cabling, fibre, connectivity details, power and earthing requirements
33. Servers/Storage hardware maintenance and support is based on various maintenance levels.
34. Alert the contracting party about hardware changes that may impact application execution in support of the UDI's application testing.
35. Design back-out processes to return to the former hardware configuration if unforeseen problems occur during installation.
36. Co-ordinate the scheduling and installation of supplier- recommended preventative maintenance and other hardware specific changes.
37. Schedule down time as and when required to perform required hardware preventative maintenance, installation and testing.
38. Design, build, schedule, and implement a hardware refresh template.

39. Configure operating systems at the setup of each server, to establish super user privileges and access rules and establishing other standard guidelines, based on the agreed security policy of the contracting party
40. Establish the process and procedures for requesting logon IDs and OS system level access
41. Create, modify, and delete system logon IDs using the Change Control Procedure
42. Monitor and maintain accounts and IDs and their designated privileges or access to make certain only active, authorized IDs have access, based on the agreed security policy.
43. Remove inactive or suspended IDs after a specified amount of time, based on consultation with security administration and the contracting party using the change control procedure
44. Adjust and maintain operating system and security software parameters for password expiration, available in the specific operating system environment to meet the agreed security policy requirements
45. Provide processes and procedures to maintain operating system data protection options.
46. Perform bi-annual re-verification of data owners, authorized submitters and logon IDs, existing level of privileges, based on input from the UDI and system security configuration.
47. Work with the UDI's application support personnel as reasonably required for the Quarterly reviews and maintenance of inactive user id's
    - Compile a list of defined users id's on the Operating System, and provide list to the UDI
    - Perform reviews of system, monitoring and database administration user id definitions.
    - Bidders will apply the necessary changes as per the outcome of the review.
48. Hardening of servers as per UDI's requirements
49. Anti-virus scan and anti-virus update on the server
50. Bidders will delete the UDI's application user id definitions, once such a request has been forwarded by the contracting party.
51. Bidder to update virus related signature files on servers to manage the removal of malicious code.
52. Support and ensure that the timely installation of updated signature files and anti-virus software patches on all servers within the managed environment occurs.
53. Coordinate with UDI's SOC Vendor for receiving the most up-to-date information on malicious code outbreaks and the appropriate software signature files to protect against malicious code.
54. Obtain and release signature files for testing and application into a client dedicated environment.
55. Signature file and patch updates to be made available and installed utilizing the UDI's change control process.
56. Testing of signature files are to be performed prior to deployment.
57. Perform pre-production scans to identify potential security risks on a server prior to entering the production environment.

58. Review the results of vulnerability scans and determine corrective actions based on the results of the scans
59. Review the results of penetration testing and determine corrective actions based on the results of the scans.
60. Review government and supplier bulletins and various other sources to identify emerging threats or vulnerabilities to the UDI's hosts.
61. Maintain the risk evaluation process of vulnerabilities in which mitigation plans are determined, in accordance with the agreed security policy.
62. Maintain a vulnerability correction process to correct vulnerabilities detected through scanning of servers.
63. Maintain a vulnerability correction process as new vulnerabilities are identified.
64. Correct known vulnerabilities detected within the scope of the bidder's responsibility, using the appropriate correction and change management processes.
65. The agreed security policy is to form the basis of security level.
66. Maintain processes to provide consistent configuration of parameters for logging devices and ongoing maintenance of those parameters.
67. Make certain of adequate retention of security event logs, based on the agreed security policy.
68. Configure the parameters of the administrative tools for all system hosts, in accordance with the agreed security policy.
69. Will provide event logging to the extent that tools, resources, and storage are available on client owned environments
70. Ensure sufficient storage capacity available to retain logs
71. Provide a listing of resource access rules for re-verification purposes
72. Perform quarterly review all user ID's and forward list of ID's not used for the last 6 months to the contracting party for permission to delete these ID's.
73. Process security data identifying logged or audited access to a resource.
74. Process security data identifying attempted access to a protected resource.
75. Process security data identifying password violation attempts.
76. Process security data identifying usage of emergency ID's.
77. Monitor and maintain ID's and their designated privileges or access to make certain that only active, authorized ID's have access.
78. Adjust and maintain operating system and security software parameters, consisting of password expiration, available in the specific operating system.
79. Provide performance management functions and establish performance monitoring thresholds for major processes.
80. Proactively identify performance problems and improvements.
81. Provide capacity planning processes, for short term and long-term planning, forecasting resource requirements, and analyzing and reporting resource trends.
82. Monitor server utilization, CPU usage and I/O activity, produce capacity projection reports and develop plans for improvements.

83. Review server capacity and advice where future additional capacity may be required or archiving policies need reviewing or implementing.
84. Use standard operating system utilities and/or other third-party tools where appropriate, to project the effects of new changes and workload changes or when large configuration changes are performed in the environment on request of the contracting party.
85. Perform operating system software tuning \ optimization as required to maintain day-to-day operations
86. Provide, install and maintain performance monitoring software.
87. Maintain system parameters to manage subsystem performance and workload throughput.
88. Implement changes as necessary to optimize the effectiveness and efficiency of the server platform.
89. Analyze system resource and storage utilization.
90. Perform capacity trend analysis.
91. Perform capacity modelling.
92. Capture capacity usage for the last 12 months.
93. Provide forecasting based on historic trends and planned UDI's initiatives.
94. Provide assistance with batch scheduling issues and problems using the problem management process.
95. Process job dependency information for batch job cycles as defined by the application support staff.
96. Maintain specific batch cycles utilizing the standard operating system CRON scheduler throughout the operational support coverage hours as necessary to meet defined service levels.
97. Provide appropriate system resources, tools and procedures to support the processing of user-initiated batch jobs.
98. Agree with the UDI prioritization for scheduled, ad hoc and system jobs.
99. Provide the necessary operational resources to support UDI-submitted or UDI-scheduled batch processing.
100. Maintain tools and facilities for UDI to perform batch scheduling and batch monitoring activities.
101. Log problem records if scheduled and automated batch jobs fail.
102. Consult with the contracting party should job priorities require a change due to system constraints.
103. Perform problem diagnosis and purging of jobs on Operating System as necessary.
104. Monitor automation tools and functionality.
105. Maintain and execute system start- up/shutdown processes.
106. Monitor, identify, and implement automation techniques to remove manual interventions for ongoing monitoring and operation activities.
107. Perform maintenance and support for automation tools and products
108. Problem determination and isolation for automated operational processes.

109. Maintain and update documented hardware, facility, operating system, database and related system software recovery plans as necessary.
110. Perform quarterly tests of the recovery plans to verify the effectiveness there-off in supporting the day-to-day UDI operations.
111. Provide the required personnel resources to perform recovery plan drills or actual recovery plan execution at the time of disaster.
112. Provide requisite mirroring and redundancy across the DC & DR facilities to ensure adequate failover for the server environments.
113. Cluster configuration including the integration of startup/shutdown scripts
114. Configuration of shared storage
115. Provision of documentation on implemented high availability solution
116. Installation, maintenance and monitoring of clustering
117. Conduct Cluster tests as a part of DR drills

5.5 Storage Management

Storage and data consist of a system managed storage strategy that enables all data to be managed individually and automatically by the system. Within the system managed storage environment are both online and removable storage media, commonly referred to as disks and tapes. UDI requirements for data availability, accessibility, performance, and retention can be accommodated at the data set level and used by the system managed storage environment to select the correct media.

The expected storage and data management services can be further defined by the following high-level service requirements:

Service	Description
Mirroring	Includes the management of the SAN environment to ensure the availability, integrity and redundancy of UDI's storage environment across DC, DR and near site
Configuration	Process of organizing and maintaining storage information to streamline the process of maintenance, repair, expansion and upgrading.
End to end storage monitoring	Continuous monitoring of a DC&DR Storage Equipment notification to the administrator(s) in cases of failure / outages.
Archiving	Assist in implementing and maintain UDI's archive strategy as part of ensuring effective usage of storage resources.
Media management	Management of the associated media and peripheral equipment used for data storage (e.g. tape management)

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines
2. Develop and document storage and data management requirements and policies.
3. Develop and document procedures for performing storage management that meet requirements and conform to defined policies
4. Review Storage Management procedures on a regular basis to be defined.
5. Provide appropriate data storage services (e.g. RAID array, SAN, tape, etc.) compliant with the agreed service levels and performance and availability metrics
6. Monitor and control storage performance according to data management policies.
7. Maintain and improve storage resource efficiency and space requirements.
8. Perform data backups and restores per established procedures and service level requirements as well as in accordance to the UDI's change management process.
9. Adjust the backup and restoration plan as new components are added to the system or availability requirements change
10. Provide input processing, for activities such as loading and rotation of third-party media (e.g. tape) and receipt and/or transmission of batch files, or large files.
11. Define storage management reporting requirements
12. Provide storage management reporting as defined by the UDI
13. Maintain the integrity of storage media, e.g. tape and disk.
14. Maintain the data integrity across DC&DR
15. Perform the relevant maintenance activities to ensure data availability and redundancy
16. Management of all third parties required to support the storage and data environment
17. Storage Management administration – manage and (Pro-active) monitor to ensure all time storage availability.
18. Resolve incident/problem related to storage as per agreed SLA.
19. Supporting new and existing storage products and services like replication, mirroring, security, traffic analysis, compression, virtualization etc.
20. Managing of physical storage elements/equipment
21. Managing moving inactive data off of production machines to free online disk space for important active data
22. Managing logical storage elements like caching, I/O technologies, data protection technologies etc.
23. Storage provisioning. Estimate and recommend storage requirements
24. Performing data management including backup and recovery
25. For disk storage, responding to storage requests by:
    - Allocating raw storage
    - Defining logical volumes
26. Troubleshooting disruptions and working with vendors to resolve the issues including software/firmware/patches related issues
27. Performing capacity management of storage resources to meet business needs
28. Planning for upgrades to hardware and software (including execution)

29. Granting UDI access to the storage management system from all applicable locations where the Services are performed, and allowing UDI to monitor and view the knowledge database on an ongoing basis (including Authorized Users)
30. Storage provisioning, purging of disk space, Replication support, LUN, SAN Switches, FC Links, Point in time copy / Snapshot management, RAID Configuration
31. Supporting Disaster Recovery activities pertaining to storage devices
32. Enable Proactive monitoring to ensure Minimal/Zero system disruptions/performance issues/outages.
33. Incorporate takeaways from Major Incidents into monitoring to prevent repetitions.
34. Maintaining documentation of configurations (including pictorial representation of the storage layout.)
35. Maintaining documentation of storage component details including architecture diagram, policies and configurations and the same should be reflected in the Configuration Management Database (CMDB)
36. Performing any other day-to-day administration and support activities

5.6 Backup and Restoration Management services

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines, the Bidder shall define data backup and recovery requirements. These requirements should cover the following at a minimum:

1. Identify the data backup technique which best suits the needs of UDI for in scope application /database/ server
2. Install, configure, test and manage any tools that may be required for data backup and recovery, such as those for writing the same data to multiple storage devices at the same time
3. Restore data to the database, as appropriate while ensuring that there is no loss of information / data.
4. Development of procedures and templates. Periodically conducting restoration drills, recording the results and reporting the results to contracting party.
5. Execute backup and recovery procedures
6. The IT MSP is required to handover the tapes to contracting party/3rd party who will vault the tapes at offsite locations and retrieve tapes from UDI's resources when required.
7. Restore required files and data sets
8. Performing mock system failure and then data restoration drills on periodic basis
9. Manage all existing and all future deployments of, Backup and Restore Infrastructure. Media will include both tape and disk drives
10. Performance tuning for the backup and restore infrastructure
11. Install and configure new equipment as required

12. Configure any new Backup and Restore infrastructure to the monitoring and alerting system and commence the monitoring activity upon completion of the installation.
13. Provide capacity planning on backup and restore platforms.
14. Equipment shifting within the premises including reinstallation/configuration and calling & labelling

5.6.1 Backup & Restoration Administration

15. Backup and restoration administration - manage and monitor backup and restoration activities.
16. Provide backup and restore infrastructure configuration maintenance
17. Handling backup (full, differential, incremental) of agreed data for all managed servers as per the frequency (daily, weekly, monthly, yearly) defined in the backup & restore policy/ procedure/ guideline by contracting party.
18. Performing media management for offsite/onsite backup
19. Handling service requests on backup and restoration.
20. Generating daily/weekly/monthly report on the backup/restoration performance
21. Performing retrieval of backup data
22. Performing back up media maintenance:
    - Defining media rotation requirements and/ or follow standard procedure
    - Labelling backup media as per backup policy
    - Planning and requisitioning of storage media
    - Monitoring and maintenance of the scratch tape pool
    - Registering tapes into automated tape handling devices
    - Handing over of tapes to UDI's personal /3rd party vendor for rotation of tapes to offsite facilities
    - Destruction of media coming out of service in accordance with back up policy
23. Executing database back-ups and restores (including export and/or import) using database tools.
24. Performing restoration activities:
    - Testing of the restore the data as per requirements of UDI.
    - Restoring complete or incremental backup as authorized (including user approval for restoration to same path, business manager approval for restoration of common folders to same path and contracting party approval for all other restorations) within 24 elapsed hours
    - Periodically verifying backup media integrity and testing of backup and restoration process as per a defined schedule
    - Restoring single or multiple objects from the backup media
25. Reviewing backup and restoration process and infrastructure, to reduce the backup or restoration windows
26. Monitoring the backup and report on backup logs. Reasons for backup failures are to be analyzed and reported.

27. Monitor tape hardware for malfunctions and monitor tape usage
28. Managing and maintaining of back up tape devices
29. Performing maintenance of appropriate documentation, in accordance with back up policy:
    - Maintaining a backup register
    - Labelling and tracking of tapes
    - Backup and verification Logs
    - Restoration Logs
30. Granting UDI access to the backup management system from all applicable locations where the services are performed, and allowing UDI to monitor and view the knowledge database on an ongoing basis (including Authorized Users)
31. Rapidly resolving every backup request/incident/problem within mutually agreed timelines
32. Backup policies configuration, modification for file systems, databases on heterogeneous operating systems
33. Performing any other day-to-day administration and support activities
34. Perform periodic audits to ensure the proper cataloguing of media
35. Review compliance with physical specifications, retention periods and Security
36. Provide monthly reports of retired and disposed Tapes. The report is to also to account for the status of all the backup media in the storage, including new media added for the month.
37. Maintain the integrity of the tape library system
38. Monitor tape library for reliability and minimization of read/write errors during the entire retention period

5.6.2 Backup and Recovery - Restoration testing

39. Carry out mock restoration tests
40. Decide applications and data for testing through restoration testing as per UDI requirement
41. Document test plans and results
42. Delete data from test servers
43. Review restoration test results
44. Storing backups and managing media life expectancy for storage media, etc.

5.6.3 Offsite Media Management

45. Responsibility for off-site media storage, including:
    - Integrity Checking
    - Compliance with UDI and/or government requirements
    - Handover the Tape Media and business recovery-related paper documentation to contracting party/3rd party vendor for secure off-site vault storage
46. Follow off-site Tape Media storage procedures, including:

- Prepare media for off-site storage, for transfer to other Third Parties/UDI's personnel as requested by contracting party, or as otherwise required
- Log all physical tape media in and out of the data center and/or remote locations, as appropriate.
- Handover the tape media to UDI personnel/3rd party vendor to ship/receive tape Media to and from the off-site storage location(s) on a daily basis or as required.
- Maintain the rotation of the tape Media that is required for off-site storage.
- Periodically Audit the off-site tape storage facility for compliance and control procedures and provide reports of such audits to UDI.
- Maintain the integrity of data shipped to off- site storage by UDI's personnel/3rd party vendor
- Notify UDI of any problems
- Design an emergency tape Media return process and submit to UDI for approval
- Comply with, and review compliance with, physical specifications, retention periods, and security

  Wipe/erase the data and configuration information resident on the External Storage Media using recognized industry standards prior to disposing of the External Storage Media.

5.7 Cross Functional Services

Over and above the defined scope of services within the domain services, it is expected that the bidder provide the IT support service management activities required to effectively manage the services required in a consistent, efficient and reliable manner and is able to meet the desired service levels.

The Cross Functional Services are mentioned below:

Service	Description
Incident management and IT Infrastructure Support Services	Incident management refers to an unplanned interruption to an IT service or a reduction in the quality of service. The objective of incident management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user. The Bidder is expected to assume accountability for the resolution of incidents as part of the 1st line of support to be provided. All 2nd level support will be the Bidder's responsibility. The Bidder should also take into account that a 24x7x365 support service is required. Bidder will raise tickets with respective OEMs for level 3

Change Management and release Management	Change management will protect the production environment and its services. All changes to configuration items must be carried out in a planned and authorized manner. This includes identifying the specific configuration items and its services affected by the change, deploying the change, testing the change on UAT environment, and having a roll back plan should the change result in an unexpected state of the service. Release management will take a holistic view of a change to an IT service and to verify that all aspects of a Release, both technical and non-technical
Service Level Management	Service Level Management will maintain and gradually improve business-aligned IT service quality through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service
Security Management	Security Management will ensure compliance to security policies, contractual requirements, regulatory/statutory requirements, and as expressed in the Service Levels
Patch Management	Provide patches management services for in-scope infrastructure at DC&DR
Software License Management	Manage compliance with all software licenses by monitoring and auditing all software use, regardless of financial responsibility for the software.
IT service continuity and Disaster Recovery	Supporting disaster recovery activities in scenario of a disaster and to keep the UDI disaster recovery plan up to date

5.8 Change Management and Release Management:

As part of the change management process the bidder is expected to perform the following activities:

In case of changes required to application software maintained by the bidder, the bidder, should collate the relevant information to assist contracting party in analysing the change request based on the following:

- Criticality and need for program change
- Exploring new ways of getting the same functionality within the existing set up
- Building workarounds
- Effect on other modules/ menu options/ business process – Impact Analysis
- Any possible effect on existing control procedures

The requirements could relate to changes required in the operational infrastructure to support new/existing requirements or frequent error messages indicating that some parts of the programs are incorrect.

The requirements could relate to additional features required to be built in the system or changes forced by the regulatory body as well as suggestions from the stakeholder community

Document and classify proposed changes to UDI services. Documentation shall include UDI cost and risk impact if needed and back out plans for all proposed changes.

Schedule and conduct regular change management meeting to include review of planned changes and results of changes made.

Modify configuration, asset management items and service catalogue (if applicable) to reflect change. Asset management is reviewed quarterly but also can be requested on demand (referred later). Disaster recovery impact is covered under the normal change control processes.

Monitor changes and report results of changes and impacts. Conduct user acceptance tests as required.

Two personnel to be considered as full-time resources for the project. Costs for the same to be factored into the solution pricing.

5.9 Service Level Management

The objective of the service level management process is to manage and maintain the quality of IT services delivered to UDI's end users. The process should also seek to improve the quality of service delivered to the end users by reviewing the level of performance achieved by the IT Help Desk.

The Bidder is expected to design and implement a service level management process to enable both the end user and the vendors to have a clear understanding of the expected level of delivered services by documenting these goals in formal documents.

The SI is expected to perform the following activities in relation to service level management with other IT processes:

1. Incident management service assists service level management by:
    - Monitoring and reporting on threshold breaches in agreements and notifying support officers when escalation and breach events occur
    - Providing information on historical data and trends
    - Providing the interface with customers on the level of services provided
    - Recording escalation actions and activities to maintain the service commitment under an SLA with the customer.
2. Problem Management service - assists Service Level Management by:

- Identifying the underlying cause of incidents and problems to minimize their recurrence
- Providing statistics, trends and historical data and assisting with service level management reporting.

3. Change management service assists service level management by:
   - Providing information on the effect of changes on the IT infrastructure and the impact on service level targets before and after these changes are implemented
   - Tracking improvement in services since service levels are defined
4. Configuration management service assists service level management by:
   - Identifying the services affected by faulty configuration implementations
   - Identifying components/functions that combine to deliver a business function/service so that underlying agreements can be set up.
5. Assess and collate the service levels across multiple vendor contracts
6. Define, document, and implement a process to ensure that service levels are tracked
7. Develop a process by which reports are produced showing the performance of a service against its SLA
8. Undertake routine exercises whereby each SLA target is analyzed
9. Define, document, and implement a process that ensures that SLAs are regularly reviewed to ensure that they meet the UDI's requirements
10. Track the SLA in conjunction with the change management process, define, document and implement a process whereby all changes to SLAs are agreed upon and raised through the change management process using a request for change.
11. Provide periodic status on the service levels maintained across all the components/services that are required to be tracked
12. Compute the penalties based on the service level defaults
13. Collate the required documentation, evidence required to be shared with the respective Vendors

5.10 Security Management:

The Bidder must ensure that the ongoing operations adheres to UDI's security policy. The Bidder is expected to monitor and report any deviation from UDI's policies for the complete operations solution.

UDI's policies are in line with global standards like ISO 27001. Audits will be conducted by contracting party (or by auditors and/or consultants empanelled by contracting party for the purpose.) Any findings unearthed during these audits will have to be fixed by the bidder. The bidder is required to ensure anti-virus scans and updates for the in-scope infrastructure.

The Bidder shall define a standard operating environment for UDI's IT infrastructure based on UDI's requirements. It shall also ensure that the required updates are performed as necessary.

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines

1. Entire in scope IT infrastructure of the UDI complies with the Security Policy
2. Activities that would be carried out:
   - user ID creation / deletion,
   - password setting / resetting,
   - Handling access
   - creation of limited access shared space on servers,
   - secured installation of assets, secured backup tape storage,
   - destruction of data on failed hardware components (for example, data on a server hard drive that fails) and
3. Confidential data protection methodologies.
4. Secure network resources against unauthorized access from internal or external sources.
5. Provide and maintain virus avoidance, detection, and elimination software for Servers.
6. Restrict physical access to Servers and infrastructure devices and other secured areas to authorized personnel only at DC and at DR
7. Implement controls which protect printed output and portable storage media (for example, tapes and disk packs) from unauthorized access and
8. Anti-virus scan on the in scope infra

Security Incident Reporting

9. Report any significant computer security incidents occurring on any systems
10. Report any significant network security incidents occurring on any systems
11. Track the number of security incident occurrences resulting in a user's loss of data integrity, denial of service, loss of confidentiality or that renders the user(s) unproductive for a period.
12. Facilitate meetings with the contracting party
13. The cloud security would consist of the following layers:
    - Cloud security governance
    - Cloud security operations
    - Core cloud security capabilities
      privacy

5.11 Cloud Security

5.11.1 Cloud Security Governance:

MSP/ CSP should be capable of applying specific policies, principles, standards and guidelines to secure data and application deployed in the cloud. These policies and standards are to be applied with existing IT governance policies of the Government / contracting party and not to be introduced in isolation.

5.11.2 Cloud security operations:

Cloud Security Operations to be able to meet the five-step process (Prepare, Prevent, Detect, Respond, Recover) under which various categorizes exist. Intrusion Detection & Prevention, Risk Assessment & Audits, Vulnerability Scanning and Remediation, Patch Management, Incident Response and Management, Investigation and Forensics.

5.11.3 Core Cloud Security Capabilities:

Identity & Access Management

(Multifactor authentication, directory services, role base access control , single-sign-on (SSO) by adapting Identity-as-a-Service (IDaaS) for implementation of single sign-on), CSP to restrict the use of root and generic accounts for Cloud Management and operations, CSP to restrict the use of root and generic accounts for Cloud Management and operations, Zero trust IT security model that requires stringent verification of identity for each device and person trying to access resources on a private network, regardless of their position within or outside of the network perimeter to be implemented

5.11.4 Infrastructure Protection

One of the most critical aspect of any cloud deployment is protecting the underlying infrastructure (compute, network, storage) from any security threats. MSP/CSP to have state of art Security Operations Centre (SOC) facilities for monitoring and managing their deployed infrastructure.

5.11.5 Privacy

MSP/CSP to ensure encryption of data in rest and in motion, key management to manage, create and protect encryption key and manage encryption and decryption tasks, data integrity and data handling are addressed to meet any regulatory or departmental compliances. Virtual private cloud for logical separation of infrastructure (server, storage, network) from other offerings of the cloud service provider with strong/robust tenant isolation to be ensured.

5.11.6 Data security in cloud

Encryption is key to protect and secure data in transit and data at rest. The following best practice to be adhered by the vendor/SI/MSP/CSP

- Multiple type of encryption to be implemented by CSP (i.e. Full Disk Encryption (FDE), Format Preserving Encryption, (FPE) Application layer Encryption, File Encryption, Database Encryption, etc.)
- For protecting data in transit, choose encryption of sensitive data prior to moving to cloud and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit for protecting data at rest, Departments can simply encrypt sensitive data prior to storing them.
- Managed encryption options through HSM/KMS. Encryption key management to maintain controls of all private / public encryption keys

- Extra layer of data security via implementation of data classification (restricted, confidential, sensitive and unclassified).
- Ensure integrity of data while replicating from one site to another.
- Backup (full, incremental, differential) data regularly to ensure availability of data and perform periodic recovery operations to check correctness.
- Ensure data-level monitoring is in place, and logs meet all the compliance requirements, if any, of the department.

5.11.7 Web application security

MSP/CSP/SI/Vendor to ensure web application security by protecting web apps and services available over internet and accessed through a browser by implementing web application firewall to protect web applications by monitoring and filtering HTTP traffic between a web application and the Internet.

- To protect the web applications from attacks such as, cross-site-scripting, SQL injection, file inclusion, as cross-site forgery, weak authentication and session management etc.
- Segregation of application access and use of DMZ (Demilitarized) zone.
- Build security while initial design process of application.
- Application integration and information exchange to happen over secured API channels.
- Security controls for interfaces and API's
- Log and monitor API calls.
- Use software-defined security to automate security controls.
- Use event-driven security such Anti-virus, when available, to automate detection and remediation of security issues. Adopting security while designing the application through the process of DevSecOps is to be ensured for application security in the cloud.

5.11.8 Cloud Security Design Principles / considerations

The vendor/System Inegrator/ MSP/CSP to ensure the following the key design principles for Cloud technology adoption:

- Security at all layers: Ensure robust Security is applied to all layers (physical, network, data, application, etc.) of their architecture with multiple security controls. This will ensure end to end protecting of application/data hosted by departments on Cloud platform.
- Safeguard data while at rest and in transit: identify and classify the data in terms of criticality/sensitivity and define their levels. This can be prevented via using the available security controls like access control, tokenization, encryption, etc.
- monitoring and auditing: ensure monitoring, auditing and alerting is configured to capture the changes in the department's system in real time. Further, log integration and metric collection can automatically investigate, act and respond.

- Access management and Controls: Ensure implementation of principle of selective privileges and impose segregation of duties with appropriate access and authorization. Centralized identity and access management can eliminate any unauthorized access and information loss/theft.
- Readiness for security events: Department/CSP needs to prepare system for any unusual security event. Regular vulnerability and security tests need to be conducted to identify the security gaps and issues. Several drill can be conducted to record the response of the Cloud systems at different layers.
- Automate security best practices: Automating software/hardware/Application based security system via AI/ML/Bots to improve the ability to secure environment which can perform regular checks and implement the controls needed to restrict the attack and enhance cloud security.
- Cloud Vendor Lock-in: Departments to ensure that there is no vendor lock-in by cloud services provider while hosting the application/data, as there are no standard guidelines between different cloud providers for data migration and exports, so it becomes difficult to migrate data from one cloud provider to another or migration to on-premise Data center.

5.11.9 Perimeter and Physical Security

Ensuring perimeter security and physical security of the data centre, shall be the responsibility of the CSP, and in accordance with the norms laid down for empanelment for Cloud Service Providers by MeitY. Unauthorized personnel gaining access to the data centre shall result in a compromise and the CSPs are responsible to ensure sufficient measures such as security guards, secured fencing, security scanners, biometric access, CCTV surveillance, Access Logs etc. are available at the data centre to prevent unauthorized or forceful entry into Data Centre premises.

5.11.10 Network Security

- CSP to implement strong security controls for internal and external network separation / communication.
- CSP to ensure appropriate network segmentation which separates networks of different sensitivity levels.
- Use Virtual Private Network (SSL or Site to Site) to access Cloud infrastructure and services.
- Use IP Whitelisting to allow connections from certain IPs and deny all others where applicable. Pre-certifying additional VLAN, firewall ports and load balancers.
- Separate virtual networks and cloud accounts.
- Restriction of traffic between workloads in the same virtual subnet using a firewall policy needs to be followed whenever possible.
- Dependency on virtual appliances that restrict elasticity or cause performance bottlenecks needs to be minimized.

- Implement policies and internal security controls to prevent traffic monitoring without approval or outside contractual agreements and consumer networks modifications.
- An automated response to attacks should be configured and additional information on the intrusion must be acquired. IP blocking, connection termination and signature analysis are some of the processes under such an automated response.
- Regularly monitor network traffic logs or implement a SIEM to get real-time security alerts generated by application and network devices.
- Prefer use of SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.

5.11.11 Host/ Compute security

- For critical workloads ensure High Availability at all deployment levels – compute, firewall, Load balancers.
- To ensure that as soon as the new application server is deployed, security scans should be enabled, and the servers should be added to continuous monitoring.
- Integrate security testing and policies while VM image creation.
- Disable remote access post application configuration.
- Implement appropriate role-based access controls and strong authentication for all Virtual Machines (VM), Containers and VM images.
- Employ the use of pre-certified VM images from the cloud platform where precertification would be an on-going effort.
- Prefer Patching of VM images rather than patching running instances. Ensure patching is up to date for Operating System, Database licenses etc.
- Ensure VM level encryption through Bitlocker, LUKS etc. for security of VM in case of compromise
- Ensure Operating System Hardening is performed on the virtual machine.
- Take periodic VM snapshots and save in a secured repository.
- Prefer use of file integrity monitoring in order to ensure authenticated changes and detect unapproved changes to files.
- Store logs (including Audit logs) externally to workloads.
- Install Anti-virus software on Virtual Machine and ensuring periodic patching is performed. Perform periodic vulnerability assessments and penetration testing (VAPT) on Department's cloud infrastructure.

5.12 Software License Management:

The bidder shall perform an inventory of software licenses as of a date. The Bidder will develop and maintain a software license inventory data base which tracks:

1. Whether the license has been procured by the SI or by contracting party
2. Whether the license comprises entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance
3. The authorized end users who have access to the Server resources

4. Expiry of licenses and contracts.
5. Maintain software license inventory to include the licenses existing as of the start date
6. Maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance
7. Perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions
8. Periodically review of software license and maintenance agreements

5.13 Performance Management

Bidder needs to monitor the performance of core insurance application and UDI web-based platform its associated database on daily basis in working hours of the UDI. The scope of the application performance management and assurance services should include, but not limited, to the following:

1. Preventive monitoring of Application (Core Insurance and UDI web-based platform)
2. In the event of a critical Alert application experts would step in to carry out initial analysis and hand over the observations for the respective teams to action the same to prevent the event from happening.
3. Availability of senior level experts on on-call basis for critical alerts/incidents
4. Provide suggestive restoration/preventive advises as applicable to ensure stability of the environment
5. APM should minimize the application downtime and provide visibility on batch operations.
6. The APM and assurance services should provide the capability to have a deep dive analysis of infra (Web, App, DB, OS & Storage) component even post alert and reduce the MTTR on issues faced.
7. The proposed solution should provide support for in any other http, https or non-http applications and should have the ability to add environment specific custom KPI's.
8. Application Performance Monitoring and Management software should deliver L1 support from an independent third (3rd) party for the first year after implementation for 24x7 application monitoring for availability, alert management, software administration, service reporting and incident reporting and thereafter bidder can factor bidder resources for the management.
9. The L2 support should be provided by an independent third (3rd) party for the first year after implementation for analysis, remediation, software administration, reporting and incident analysis, troubleshooting and alert analysis and thereafter bidder can factor bidder resources for the management. The cost of the L1 & L2 resources should be factored in by the bidder in the Annexure 16 – Bill of material.
10. The bidder is required to comply to Annexure 15- functional & technical specifications for APM tools.

5.14 Exit Management Services

In addition to the requirements mentioned in RFP, the purpose of this section is to provide details of bidder's assistance during termination or expiration of contract and exit plan strategy for the Contracting party. Bidder also has to develop a detailed Exit Plan within 6 months of signing of contract. The exit plan has to be regularly reviewed and updated on a yearly basis.

Following shall be covered as part of the Handover & Transition of Services at the end of contract period or in the event of termination. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with requirements specified herein and any statutory or regulatory guidelines

1. If any other agency or service provider is selected for providing in-scope services, the Bidder selected through this RFP shall provide support for necessary handholding, transition, sharing of information and relevant documents and other related support to the complete transitions up to satisfaction of the Contracting party. In case if the contracting party observes a lack of willingness to manage transit/ sharing of information or lack of support from bidder (selected through this RFP), they shall have absolute discretion to apply requisite penalties and deduct the amount from its billing or from performance guarantee.
2. Bidder shall provide the necessary transition for the period of 6 months. However, this period of transition could vary depending on need and the same shall be communicated.
3. During transition phase, the Successful Bidder shall not change or remove their key resources at any locations to enable the successful transition. In case such instances, the contracting party will have right to penalize the Bidder appropriately.
4. During transition phase, the contracting party will deploy a dedicated Transition Manager to enable the successful transition.
5. During the exit management process, it is the responsibility of bidder to address and rectify the problems identified with the IT infrastructure of this project including installation/reinstallation of the system software, Databases etc. The Successful Bidder shall ensure that the infrastructure is handed over in an operational condition to the satisfaction of the contracting party.
6. The ownership of the assets (including soft and hard components existing and procured through this RFP) except for those which are taken as a service, at any point of time during the term of the contract or expiry of the Contract, shall rest with the contracting party. In addition, any information/ data gathered or generated by the Successful Bidder during the term of the contract would be the property of the contracting party and the same should be handed over in native format at the end or termination of the contract.

7. In case the contracting party decides to withdraw any services/components from the Bidder's scope of work during the contract period, the Successful Bidder has to facilitate the transition of that service/components in compliance with above clauses.
8. Bidder shall provide the Termination/Expiration Assistance regardless of the reason for termination or expiration
9. Bidder shall ensure full and timely compliance with the Exit Plan
10. Bidder shall not make any changes to the Services under this Agreement and shall continue to provide all Services to comply with the Service Levels;
11. The bidder should perform a complete reverse transition of services to the new vendor selected.
12. Bidder shall within ninety (90) days of the Signing Date, deliver to the contracting party a plan specifying the Termination/Expiration Assistance including the functions and services of Bidder necessary to accomplish the transfer of the responsibility for the services from bidder to the contracting party or a Third Party, in the event of the expiry of the term or the termination of this agreement. The plan shall at the minimum, contain the bidder's detailed plan for operational and knowledge transfer requirements and list of documentation
13. The exit plan shall be updated by the bidder on an annual basis in accordance with the requirements and delivered to the contracting party project team for its approval on or before the start of each contract year.
14. Knowledge transfer and handover of services
15. Bidder shall provide for a transfer of knowledge regarding the Services to the project team personnel or designated third party personnel, including training in the performance of the services that are to be transferred
16. Bidder shall train personnel designated by the contracting party and/or its designee(s) in the use of any processes or associated equipment, materials, systems or tools used in connection with the provision of the services as needed for such personnel to assume responsibility for performance of the services
17. Bidder shall provide to the contracting party project team and/or its designee(s) information regarding the services as necessary to implement the exit plan, and providing such information regarding Services as reasonably necessary to assume responsibility for continued performance of services in an orderly manner so as to minimize disruption in the operations
18. Bidder shall provide the contracting party or its designee a complete copy of the software/architecture/solution IP in Bidder's possession or control and of the bidder IP that the contracting party is licensed with or otherwise authorized to use.
19. Explain the change management process, problem management process, policies and procedures manual, reports and other standards and procedures to the contracting party or its designee's operations staff.
20. Provide technical documentation for software used by provider to provide the services as needed for continuing performance of the Services.

21. Identify, record and provide release levels for Software and updating such records of release levels prior to and during transition of the Services
22. The bidder shall provide assistance to UDI application or its designee in notifying third-party vendors of procedures to be followed during the transition of services
23. Ensure transfer of the Configuration Management Database (CMDB) that contains details of the data elements that are used in the provision and management of the Services. The CMDB must be in a form that can be migrated to a new environment that manages the Configuration Items
24. Bidder shall provide other technical and process assistance as requested by contracting party and/or its designee(s).
25. The vendor will not be allowed to take any UDI's IP or information.

Managed service provider functions:

The Managed Service Provider shall not delete any data at the end of the agreement from the underlying CSP's Cloud environment (for a maximum of 45 days beyond the expiry of the Agreement) without the express/explicit approval of the Contracting party. The Contracting party shall pay to the Managed Service Provider the cost associated with retaining the data beyond 45 days. The associated cost shall be arrived at based on the cost figures indicated in the commercial quote submitted by the Managed Service Provider.

a. The underlying CSP shall be responsible for providing the tools for import / export of VMs, associated content, data, etc., and the Managed Service Provider, in consultation with the Contracting party, shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition related activities.
b. The Managed Service Provider shall provide the Contracting party or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the underlying CSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:
    i. Transition of Managed Services
    ii. Migration from the incumbent Cloud Service Provider's environment to the new environment
c. The Managed Service Provider is responsible for both transition of the services as well as migration of the VMs, Data, Content and other assets to the new environment.
d. The Managed Service Provider shall carry out the migration of the VMs, data, content and any other assets to the new environment (alternate Cloud Service Provider or Data Centre) identified by the Contracting party to enable successful deployment and running of the Contracting party's solution in the new environment. Master Service Agreement - Procurement of Cloud Services
e. The format of the data transmitted from the current CSP to the new environment identified by the Department should leverage standard data formats (e.g., OVF, etc.)

whenever possible to ease and enhance portability. The format shall be finalized in consultation with the Contracting party.

f. The Managed Service Provider shall transition Contracting party's solution including retrieval of all data in the formats approved by the Contracting party.

g. The Managed Service Provider shall ensure that all the documentation required by the Contracting party for smooth transition (in addition to the documentation provided by the underlying Cloud Service Provider) are kept up to date and all such documentation is handed over to the Contracting party during regular intervals as well as during the exit management process.

h. The Managed Service Provider shall transfer the organizational structure developed during the term to support the delivery of the Exit Management Services. This will include: a. Documented and updated functional organization charts, operating level agreements with third-party contractors, phone trees, contact lists, and standard operating procedures. b. Physical and logical security processes and tools, including catalogues, badges, keys, documented ownership and access levels for all passwords, and instructions for use and operation of security controls.

The Managed Service Provider shall carry out following key activities, including but not limited to, as part of the knowledge transfer:

i. Preparing documents to explain design and characteristics
ii. Carrying out joint operations of key activities or services
iii. Briefing sessions on processes and documenting processes
iv. Sharing the logs, etc.
v. Briefing sessions on the managed services, the way these are deployed on Cloud and integrated
vi. Briefing sessions on the offerings (IaaS/PaaS/SaaS) of the underlying Cloud Service Provider

i. The Managed Service Provider shall transfer know-how relating to operation and maintenance of the solution, software, Cloud Services, etc.

5.15 Cloud Management Platform-

Cloud Management Platform (CMP) would be the centralized access point to manage Cloud deployments and would act as an interface to provision cloud-based IT Services. CMP may provide facility to manage the deployment and operation of applications and associated datasets across cloud service infrastructures.

UDI requires a feature which allows to provision, manage, and terminate cloud services themselves through a Web UDI web-based platform or programmed service API calls. CMP is such a feature, a well-coordinated unified management framework that provides an interconnected view of the infrastructure and end-to end visibility.

The Cloud management services provides the key capabilities which are necessary for operations and management of the resources and services required by the consumer. Cloud

Management ensure smooth process flows as per business agreement and the prime objective is to maintain critical services up and running.

Cloud management comprises of the administrative tasks involved with creation, maintenance, product/service performance and quality control of the environment within defined scope of work. Cloud management services focuses on processes and services invoked, such as when and where activities occur, who delivers them and how many people or entities they reach.

UDI CMP should have the ability to create monitors that actively check various metrics, integration availability, network endpoints, and more.

5.16 End to End Support

Bidder needs to provide the facility Management support to UDI after go-live of the UDI web-based platform. The annual maintenance and support services would cover all the items both hardware and software. It will be bidder's responsibility to locate the exact nature of the problem(s)/ fault(s) and rectify the same, if any, during the warranty and annual maintenance period.

UDI shall have one integrated help desk for all the initiatives being run by the corporation. This helpdesk shall be the Single Point of Contact (SPOC) for all business and IT services staff. This helpdesk will be the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. The support (L1, L2, and L3) should be available from the day the new application goes Live at any of the UDI Offices or over the internet.

The Bidder has to provide the resolution / service as per the defined service levels. The Bidder has to make sure that the methodology proposed for addressing and resolving problems is aligned to the required and defined service levels.

The Bidder should staff persons in support who are conversant with the solutions deployed and are capable of resolving routine problems and queries through the service desk application or over the phone.

The minimum number of resources are provided in the RFP however bidder needs to size the number of resources to meet the SLA.

6 Security and Performance Requirements

The Bidder shall devise the system for handling all security issues like handling authentication, role-based access control, portlet security, and web services security. The Bidder needs to secure connections between clients and the UDI web-based platform and other applications as well as connections between the UDI web-based platform and systems of all stake holders. The security plan requires to be approved by contracting parties before implementation. The

bidder needs to submit a separate paper on how the security can be implemented for the UDI web-based platform.

1. The UDI web-based platform should incorporate necessary security features against hacking and defacement.
2. The security design for the UDI web-based platform and app should follow the best practices for the websites, secured website, and enterprise UDI web-based platform/web servers as per the security policy of UDI, CERT-In/IRDAI/Government guidelines.
3. All logins and payments transaction must operate on secure protocols. It should provide support for website security audit.
4. The UDI web-based platform should comply fully with the guidelines issued from time to time by Government of India.
5. The Bidder will arrange security audit of web UDI web-based platform from one of the empaneled agencies (by CERTIn) and clear the same, prior to “Go-Live".
6. The Bidder should assist UDI to formulate a security policy to address various security issues related to web UDI web-based platform and app.
7. All development and solution proposed should be Compliance of ISNP/ISMS guidelines
8. Solution to use approved technology and meets all information security policies
9. Threat prevention, detection, and response with SIEM and endpoint security
10. VAPT/WASA
11. Encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
12. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

6.1 Encryption & Security of data store

It is to be noted that since the data store deals with insurance at a personal and individual level, it will contain personal identifiers such as date of birth, Aadhar number, driving license number, etc. With this being a prestigious Government of India scheme, the reach and extent of data entry will be large and detailed. Hence, it is very important that confidential parts of the data that is stored in the database be present in an encrypted format, even inaccessible to the admin of the system for a casual look. The data would be accessible through specially written routines and scripts for the purpose of analysis only.

Vendor’s IT servers, systems, data and network shall be:

a) always in India and shall not be outside India
b) protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data and is secure service against unauthorized entry or access
c) with standard transmission and encryption formats in order to protect the confidential information from any disruption, hacking, etc.

d) protected against loss or destruction and arrangements would be made for disaster recovery at a location different from the existing place in a different seismic zone.
e) equipped with robust firewall, intrusion detection, data encryption, disaster recovery, DDOS and other internet information security management systems and any other systems that are needed to satisfy the requirements which shall not be less than the reasonable security practices and procedures as prescribed under Information Technology Rules, 2011 (Reasonable security practices and procedures and sensitive personal data or information) or any amendments/modifications thereof, and failure to implement such reasonable security practices and procedures shall result in not only the contracting party proceeding to take suitable steps/action against vendor, but also vendor shall make itself /himself liable to pay damages by way of compensation to the person so affected.
f) adhering to ISO 27017 cloud security guidelines and achieving similar certification for this repository.

6.2 Data security & confidentiality

Since the data confidentiality and privacy of data is of utmost concern, adherence and following of the norms as prescribed under the GDPR is essential. (Reference to the Personal Data Protection (PDP) bill expected to be enforced in the near future may also be taken). All steps to be undertaken to guard the data against malpractice, and leakages – by hackers, by manual means or through employees or even database admins should be listed and explained. The ***various security features and technology enabled measures that are recommended to ensure privacy, strong means of authentication, identification criteria, trust and multiple verification mechanism*** should be highlighted, and the proposed plan explained in the proposal.

Since the datastore will be accessed by system admins and data specialists of the member companies as also users of the UDI team, the Government of India officials and the members of the vendors working on analysis of the data, from multiple locations and through various methods, it may be explored whether a ***key vault or the LDAP protocol*** can be incorporated. The key vault or LDAP/ active directory incorporation into the overall architecture for access, and the list (types) of keys that it would contain, and features to be used to be elaborated upon.

Since the solution is going to be cloud based, BYOK (Bring Your Own Key) concept is to be incorporated so that the data at rest can be encrypted at the cloud end using the key provided by UDI. The same to be elaborated in the technical solution.

Aadhar data has to be stored in Aadhar vault or as per the current Aadhar regulations.

The database should be capable of segregating data as per ownership, with the intention of maintaining security.

6.3 System Integration Testing

The UDI will require the successful bidder to prepare a plan that details the methods and procedures that will be used to execute the test cases. On completion of unit testing of all modules by the UDI web-based platform and app developer, the testing team will carry out a complete integration testing. During the SIT run, all the transactions and features will be verified along with interaction with all other external applications. The test run methodology will be developed and adopted after consultation between the bidder and the contracting party. The bidder will also conduct a Stress & Performance Testing of the UDI web-based platform and app as per the load mentioned in the RFP before deployment of the solution for production. The benchmarking and stress testing are detailed in the RFP.

Bidder needs to submit the result and test cases used to do the Unit testing and SIT before starting the testing by the External agency. During SIT and Unit testing bidder needs to execute both positive and negative type of test cases.

The bidder is expected to carry out periodic security and penetration testing on the UDI web-based platform and solution and submit its report to contracting party to ensure that the solution cater to the expected load specified in the requirement. Tool for doing the security and penetration testing should be provided by the bidder.

As part of testing user needs to perform below:

1. System integration testing
2. Performance Testing
3. User acceptance test support
4. Application Security Testing
5. Regression Testing
6. Defect fixes
7. VAPT/WASA
8. DC-DR Testing

6.4 Application Performance Management

The bidder is required to design, size, supply, implement and maintain application performance management and assurance tools or such an equivalent that would help monitor the UDI web-based platform. Bidder needs to procure, implement, maintain the required server hardware, storage, operating systems and databases for the tools. Any other software & hardware required by the bidder for APM tools needs to be procured and implemented by the bidder.

The scope of the application performance management and assurance services should include, but not be limited, to the following:

1. Design, size, supply of software and hardware, implementation, monitoring and management.
2. Preventive monitoring of mentioned applications

3. In the event of a critical alert application experts would step in to carry out initial analysis and hand over the observations for the respective teams to action the same to prevent the event from happening.
4. Provide suggestive restoration/preventive advises as applicable to ensure stability of the environment
5. Minimize the application downtime and provide visibility on batch operations.
6. The APM and assurance services should have the capability to have a deep dive analysis of infra (Web, App, DB, OS & Storage) component even post alert and reduce the MTTR on issues faced.
7. The proposed solution should provide support for any http, https or non-http applications and should have the ability to add environment specific custom KPI's.

6.5 Database Access Controls

The usage of PIM to ensure role segregation & recording of Privileged access is preferred.
The details of the actual solution may be expanded in the proposal submitted. The ***Database administrator and the system admin will also have only read only access*** to the actual data, while any backend edit/delete can only be done in extreme cases with appropriate permissions. Likewise, the network management person to also have limited access. All activities to be audited and any discrepancies to be highlighted immediately.
A yearly round of VA/PT is to be conducted and report submitted to the contracting party. Such VA/PT should be conducted by an external entity who is CISA/DISA. In addition, the vendor is expected to extend co-operation in the conduct of an external audit or VA/PT as determined by the contracting party. The responsibility of resolving the findings of the VA/PT rests with the vendor, at no additional cost.
A tool to be created for access to the data for actual transforming and correction of data.
The tools can be assigned rights and all actions done by the tool will be monitored. After a defined time-interval during which the data (including the personal identifiers) have been verified and corrected as the case may be, the entire data will be made anonymous. The personal data and health information of the customer will be masked in the database and the tool can be used to decipher the values as and when needed.
The tool should have the following features (only preferred and prescribed, the actual tool should cater to the requirements of security):

- Authorized personnel access (authentication & authorization, IP address, login, etc.)
- Separation and segregation of data access based on certain pre-defined set rules, e.g., only the data accessed by the company. Read/write access or only query with yes/no response
- Trace the attempts to access and relevant messages to be sent to the authorized persons when escalation of privileges have occurred.
- Additional layer of security for sensitive personal data.

Broadly, the steps taken as information security controls towards

- Access control
- Authentication
- Integrity controls
- Application security
- Auditing
- Encryption
- Backups
- Database Security

Need to be specified and elaborated upon with the complete schema.

Vendor should provide requisite support for auditing the security of the environment including but not limited to - security and compliance audits RED team assessments, and vulnerability and penetration testing for audit purposes. The vendor is expected to elaborate on the security standards and practices that will be implemented in the project.

7 Project Management

As part of the project management exercise, the bidder is expected to:

1. Setup the project management office
2. Assistance in project management and project delivery team identification and resourcing
3. Change management procedures
4. Project planning and detailing
5. Project quality management procedures
6. Project Manage All phases/part of the project:
7. User Acceptance testing
8. Data migration
9. Rollout
10. Closure of issues pending for resolution
11. Measure the progress made in the implementation of the project
12. Track customization and gaps
13. Monitor closure of gaps and customizations as per delivery schedules
14. Provide regular updates to the steering committee and board as required by the UDI.
15. Participate in all technical and functional discussions relating to the projects
16. The bidder is required to project manage the Go-Live and provide executive reports.

Agile methodology is preferred as a project management principle. A mixed model would be the ideal case, after Part A with the project teams working on Agile during the implementation and then on a waterfall model for the actual rollout and bug correction cycles. Note that each Part would be considered as a separate cycle and worked on accordingly.

The project teams at the bidder end and the contracting party end to work in close quarters to ensure the actionables are delivered as per the agreed timelines. Since the project is dependent on multiple stakeholders, the timelines would overlap and the UAT would also be two pronged. It should be noted that UAT would be considered complete only after a sample

set of stakeholders have tested and passed the application, and not just the contracting party project team.

Any specific roles/ skillsets required from the contracting party end may be highlighted in the project plan.

A detailed project plan with timelines is expected to be part of the bid submission.

8 Existing functionality

SBI Life Insurance developed Unified Digital Interface **UDI** application that provides a set of interfaces for the various stakeholders for e.g. banks and insurance companies for transfer and exchange of data. The application mirrors closely the requirements of the schemes and caters to the basic requirements with its existing modules.

The main objective behind this approach is to provide interface to upload, insert and update prerequisite data and documents in seamless manner to reduce the processing time. The major advantage of this application is that, the process from enrolment of the member under the scheme till settlement of the claims will be faster and seamless for the Bankers and the insurer. UDI provides the framework for a central repository of the customer, which can be referred by Bankers at the time of enrolment and Insurers at the time of claims settlement for deduplication purpose.

The Unified Digital Interface application provided by SBI Life insurance can handle the workflows for PMSBY and PMJJBY schemes.

Both schemes have largely the modules enrolment, claims, (upload through manual and bulk mechanisms) and MIS, grievance redressal. The existing functionalities may need to be suitably enhanced/ modified to achieve the objectives.

8.1 Creation of Unique Reference Number (URN) for each customer

Each new customer would be identified by a Unique reference number (URN) in the proposed application. This will be maintained and referenced for tagging with claims and for future access. The Unique identifier would also help to identify renewed policies over the years.

The data against each URN would be validated at the UDI interface with the data repository. Thereafter, the banker entering the data would also verify the customer data with his bank records in CBS database and confirm the same on the platform.

8.2 Deduplication of records

Since, there is no single approved identifier, a deduplication functionality has been built into the existing application by fuzzy search algorithm based on the weightages assigned to a set of enrolment screen parameters. Manual intervention is required for creation of URN.

8.3 Data Entry of enrolment/ renewals and claims data

As is seen in the annexure on UDI_Processflows, all the enrolment data as per the forms prescribed in the scheme have been incorporated into the application. The individual enrolment, renewals and bulk data upload has also been built in for both PMSBY and PMJJBY. Hence, data entry into the system has been completely handled.

8.4 Image or document processing

The documents provided by the customer at the time of enrolment and claims are stored as scanned images or documents in the repository and available to be retrieved as and when required.

8.5 Bulk data upload

There is a provision to upload data in bulk through excel files in a pre-defined format. All such uploads also require further reasons for updation. The bulk data upload is available for renewal of data as well as during normal enrolments and claims data entry by the banker.

8.6 Generation Certificate of Insurance (COI)

There is a provision to generate COI, which can be shared at any time with the customers. There is also a provision to notify customers through SMS in case of success/ failure

9 Requirements – Part A

9.1 Hosting

Hosting will be done and managed by the bidder. Cloud environment is preferred; however, a data center availability will also be considered. The bidder needs to ensure:

1. The infrastructure, Storage should be offered as virtual private cloud- as a service.
1. Bidder needs to note that for database, bidder is free to choose either to host the same as service from the cloud provider or manage the same on the infra which is taken as service from the cloud.
2. High-availability (active-active) for UDI web based platform and application at DC & DR
3. DC & DR set up must comply with all Indian regulatory guidelines defined for providing cloud-based services in India.
4. Since bulk of the data is expected during a particular fortnight of the year, elasticity in terms of ramping up the resources for a small period is a must
5. RTO – 4 hours and RPO - 60 mins
6. All the environment (DC, DR & Non-Production) to be hosted inside INDIA availability zone. Data Centre and Disaster Site (DR) shall be in India but in different seismic zone. No network, and data sharing/replication to any data centre outside the boundaries of the country is permitted

7. No separate charges for inbound or outbound data transfer-charges only for port hours consumed and not data transfer
8. Bidder needs to ensure that if at all during the contract period UDI wants to move any or all environment from cloud to On premises/or any other public cloud then the selected cloud and bidder should have the provision of the same
9. Bidder and cloud provider will be responsible for all time of security management like VAPT, WASA for any security breach.
10. The bidder will be bound by Indian law and Indian IT Act (Cyber Law). No data in any circumstances should be shared / copied / transmitted without UDI's consent / written permission of UDI and it should be as per the Indian IT act (Cyber Law).
11. The bidder shall propose hardware such that at any point in time during the contract period, the peak CPU utilization of compute should not exceed 70% at the Primary Data Center and Disaster Recovery Center and 80% for storage.
12. The data files along with archives and individual file storage should be hosted in India for primary and secondary copies
13. The cloud infrastructure provider should have presence in at least 2 cities in India
14. The bidder must provide the Application Deployment Architecture with diagrams, identifying components and specifications for each component with description. Description must detail the number of servers, specifications for each resource (Web server, Application, DB, File server, Resource Monitoring servers etc.), Operating System and configuration as well as function of each server, Network Bandwidth Requirements and Storage Requirements.
15. The bidder is responsible for actual sizing of the infrastructure as per the scope of work, activities and Service Levels and projections as defined in this RFP
16. The bidder should provide sizing methodology detailing how the proposed solution architecture and sizing will meet UDI's requirements.
17. The proposed infra should be IPv4 & IPv6 compatible
18. All IRDAI and Govt. Mandated existing and future guidelines including ISNP/ISMS/Cybersecurity

9.2 Software Management (Maintenance and Enhancements)

The following considerations must be taken for supply of software:

- All software envisaged is required to be licensed to the Contracting party.
- The software supplied must be the latest version of the software supplied by the OEM.
- Beta versions of any software shall not be accepted.
- The bidder shall ensure that the software licenses supplied in its bid adequately cover the needs as per the requirements in this RFP.
- The bidder must consider the disaster recovery environment while proposing the software licenses.

- The successful bidder should provide comprehensive ATS for proposed solution, including other software, associated modules and services required to meet the requirements in the RFP.
- The support for the solution should include the following:
  - All minor version upgrades during the period of contract at no extra cost to the UDI
  - Program updates, patches, fixes and critical security alerts as required
  - Documentation updates
- The proposed Application version shall not become End-of-Support for the entire contract duration.
- All source code to be handed over to the contracting party after development. Any changes and upgrades to also be kept updated within the source code maintained at the contracting party end.
- The source code (except for proprietary solutions used) should be the IPR of the Contracting party only, to avoid vendor lock-in particularly post the project period
- Considering the voluminous data, design and development of database repository to be of such a manner, so as to extract data in the fastest and most efficient manner using URN and implementing advanced de-duplication mechanism. Also, URN needs to be generated for the historical data as mentioned in 5.2.

9.3 Data input of current active policies.

The migration of the current year data, through a bulk upload mechanism needs to be set up for immediate input into the UDI platform. The formats are expected to remain the same as the bulk data uploads. A URN will be generated and basic deduplication done by the existing application, as per the rules set for enrolments.

Hand-holding and handling problems with missing/ wrong/ change of parameters during the course of the year, to be handled by the vendor as part of the migration of current data exercise.

Planning of data architecture and data structure for the migration of current data (current policy year 2021-2022)

The data is expected to be loaded into the system in two parts – from June 2021-end Mar 2022. And then for the months of April 20220-May2022, for the FY 2021-22 enrolments.

Further any new enrolments into the system for the FY 2022-23, will be handled as a separate activity. Renewals for FY 2022-23 will be on the basis of this uploaded data, and would use the URN thus generated for upload.

Vendor to note this process and accordingly manage the system and the stakeholders.

9.4 UAT Setup and testing

The bidder will completely be responsible for end-to-end UAT and data migration audit.

Data testing on pre & post migration state of data is part of the scope. Testing agency will have to report on field level variances, if any.

Based on the contents of the RFP, Test Methodology in consultation with the UDI, based on a standard which is suitable for the UDI and perform UAT on behalf of the UDI. The external testing agency will completely be responsible for end-to-end UAT.

9.5 SMS/ email Notifications

Integration with an authorised SMS provider, with necessary permissions for generation of SMS text is under the scope of work by the vendor. The SMS provider agreement would be in the name of the Contracting party and all bills at actuals will be borne by the contracting party.

Email to be configured for sending mails to the parties would also be provided by the contracting party and will need to be integrated with the code by the vendor.

9.6 Training

All the users of the system would require detailed training on the usage of the system. In addition to formal training sessions to representatives at a pre-planned session, documents on the usage of the system and a regularly updated FAQ system would also be required.

A total of 5 training sessions can be planned for about 50 participants each.

9.7 Handholding

The stakeholder representatives would need to be supported during their activities, the helpdesk created would attend to issues and concerns, comments and suggestions from the users of the system.

Particularly for the API integration the software team would be needed to handle any issues with integration or connectivity or network. The same will be provided for with a time frame by the bidder and suitable mentioned in the proposal sent.

10 Requirements – Part B

10.1 Data Migration

The existing data of approximately more than 35 crore customers since the start of the scheme need to be migrated from the individual/banks and insurers to the repository. This would also involve

- Planning of data architecture and data structure for the migration of all data from the start of the scheme
- Planning of archive structure,
- designing templates and process,
- enabling data extraction and entry in the right format from the stakeholders
- performing appropriate quality checks on the data
- handling any missing data points as per the current rules of mandatory data
- generation of URN for the record ensuring same records on renewal retain the URN
- Deduplication of records, including, any duplicate records from historical data to be highlighted for further processing, and to provide separately duplicate claims if found.

The data migration activity would involve participating in interaction with banks and insurers to enter into the UDI platform data on enrolments and claims, and handholding to help transform the data into the formats needed by the UDI and aid in successful upload of the same. The data is to be migrated and saved with the year tagged.

The deduplication algorithm may throw up matches which will have to be tagged and handled. Also required is performance of Deduplication activity and appropriate action further.

It is to be noted that since the current year data has been uploaded into the system, the URN against the customers have been created for the older policies. The same to be mapped and stored.

10.2 Deduplication

The bidder is expected to create the database in such a way that deduplication of the data can be carried out in an efficient and fast manner. The data entered each time would be compared against all the records entered for that year and the previous year. Thus every record entered would have a match made against over 35 crore data sets. Since there is no single approved identifier, the data can be matched in various ways

Deduplication would be carried out at various levels

- Matching of specific data fields for an exact match.
- Handling variations in spelling of names and addresses
- Checking for earlier claims or accidents
- Multiple enrolments from different banks
- Checking of addresses and nominee details with a % allotment of value
- Putting forward the duplicate cases for further investigation

This functionality has been provided in the Unified Digital Interface application at a basic level but will need to be enhanced and bettered. Hence, if any pre-existing deduplication mechanism exists with the vendor, the same might be highlighted.

The response of the queries to these data checks should be within 5 seconds, at the maximum.

The set of fields used for deduplication should be easily configurable by the administrator of the system. The algorithms thus used can be modified as per the parameters set. A suitable configuration management tool for the same to be provided.

As of now no unique ID is available for deduplication and the process is semi-automated. Manual intervention is required. Hence the results of the process to be shown to the user and then an ability to accept the results and reject the entry or go ahead with the data entered should be available.

The deduplication algorithm is be such that a response to a new entry is received within 10sec.

In this part, after the initial system is ready and functioning, the linkages to the systems of the banks core banking systems and the insurers booking systems will need to be built up. The

data required in the forms as per the scheme will be extracted by entry of minimal fields. The following links are envisaged.

10.3 Search Engine

A powerful search algorithm needs to be built in to cater to specific scenarios as under:

- For Deduplication process - UDI to Repository at both workflow stages (Enrolment & Claim)
- For updating the records on various stages of the enrolment/claims - UDI to repository
- To update the Grievance & status- UDI to repository & vice-versa

11 Requirements – Part C

11.1 Configuration Management

An administrator of the contracting party would need access to the system to manage and maintain the masters as also configure auto generated tasks and reports. Such a manager from the UDI project team would have access to the data as well as be able to extract reports over the entire data.

A suitable user-friendly UI based tool for the same is sought.

11.1.1 User Management

Users for each company have been uploaded into the system. An admin user for each company (bank/insurer) to be created within the system and roles assigned to him to maintain all company related information including company branch master, codes, users.

The actual users to also be managed by such an admin user regarding the access and activation for the users under that company.

Contact detail updation and password handling to be a part of this system.

Users to be configured with read only access or with full access. Various roles and permissions to be configurable.

11.1.2 Company Management

Masters for all the stakeholders to be created and their respective branches and codes to be maintained over the duration of the project.

Mergers and acquisitions of companies to be handled. A separate module to move the policies, and handle the deduplication suitably should be built in. During a merger/ acquisition, the old data to be maintained and tagged accordingly. A suitable solution to be finalized in conjunction with the stakeholders and the contracting party project team.

11.1.3 Master data Management

All the masters used within the system can be managed by the vendor project team with due approvals from the contracting party officials. The handling of changes in the master data to be associated with "applicable from a particular date", both versions as per the cut off date to be available and linked throughout the application.

All the scripts and scheduled tasks to be configurable on the system and visible to the project team.

11.2 MIS/ Reporting

Reports will be generated from the data repository. The data available to each stakeholder with a login would pertain to details of the data that are specific to only that company/user. However generic reports at a scheme level would be available to all users.

A list of 10 reports per type of stakeholder and a set of 25 reports on a generic level can be considered for the purposes of this process.

There will also be a live dashboard indicating, among other data, the enrolments and claims on a real time basis as they are entered into the system.

11.3 Archiving

Currently, data since inception needs to be archived and going forward, all data pertaining to previous years to be archived. At any given time, two years old data should be available to handle deduplication.

11.4 Grievance Management

The application provides for entry of complaints/ grievances that will be sent as notifications to the banks/insurers or sent through the API integration with the respective CRMs. Hence the master files of reasons and contact details would need to be entered.

Monitoring of the claims/ complaints and their closure will be closely monitored by DFS and others. Hence it is important that there is dedicated follow-up and completion. For this purpose a helpdesk is proposed.

12 Requirements – Part D

12.1 APIs between UDI & stakeholder entities:

The UDI application is currently built as a standalone application which will handle the transaction flow for all policies under PMJJBY/PMSBY. This application will be used by all the bank branches, Insurance companies and personnel from DFS. UDI, as is, and covers

- Processing of transactions entered online

- Processing of transactions uploaded in batch
- Grievance management
- Management reports

Developing and exposing common standardized API endpoints through web-services to enable all stakeholders including banks and insurers to integrate seamlessly with the proposed common platform irrespective of the technology used by Banks/insurers.

As part of the RFP scope, when the repository of the PMJJBY/PMSBY universe is set up by the vendor, they are expected to seamlessly integrate the UDI application with the repository. The necessary APIs are to be built and the vendor need to work with the banks/insurance companies/intermediaries in integrating their systems with the repository and UDI such that the transaction flow as envisaged in the workflow provided, is established. This also includes any real time integration of the repository/UDI application deemed necessary with any of the government approved sourcing platforms for sourcing and supporting PMJJBY/PMSBY policies.

The data points for each of these integrations are elaborated in Annexure on process_workflows and can be further refined during the course of the project.

12.1.1 API gateway

In today's scenario Financial industry is moving towards an integrated and digital approach to all operations. For seamless, immediate and error-free data transfer, it is expected that APIs be planned. The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required tools to install the API Gateway. These would be required to be secure and encrypted.

Bidder needs to design, supply, size, maintain install and commission APIs which will be a single communication channel for use by all stakeholders as well as Core application. Bidder needs to factor all the cost of the same in the bill of material. The API will cater to the below mentioned features as well as the technical requirement mentioned in the RFP

1. Onboard new stakeholders quickly
2. Provide more secure and encrypted environment to have seamless transactions
3. Increase customer experience
4. Comply with Statutory requirements quickly and efficiently.
5. Provide a holistic view of all the API which are going out and coming in which their effective usage and more control manner

12.1.2 API integration between Bank & UDI:

- To fetch the customer data from Bank - UDI to Bank (CBS).
- To communicate the decision (rejection/acceptance of application)- UDI to Bank
- To communicate the decision (claim)- UDI to Bank
- To send payment request- UDI to Bank
- To payment confirmation/successful flag- Bank to UDI

- To update grievance in CRM – UDI to Bank
- To update the Grievance status - Bank to UDI

12.1.3 API integration between UDI & Centralized Repository:

- For Deduplication process - UDI to Repository at both stages (Enrolment & Claim)
- For updating the records on various stages of the enrolment/claims - UDI to repository
- To update the Grievance & status- UDI to repository

12.1.4 API integration between UDI & Insurer:

- For real time communication of the receipt of application and payment- UDI to Insurer
- To receive the communication for issuance of COI - Insurer to UDI
- To communicate the receipt of the claim & documents- UDI to Insurer
- To transfer claim related images - UDI to Insurer
- To update Claim settlement confirmation and payment details - Insurer to UDI
- In case during claim settlement or during enrolment, the status (requirement, on hold, etc.) update to be done: Insurer to UDI & vice-versa.
- To update Grievance in CRM – UDI to Insurer
- To update the Grievance status - Insurer to UDI

12.2 Data from other channels

Data of enrolments and renewals got from other sources such as online mean, web browsers, mobile applications etc will currently be integrated with the CBS and then moved as a bulk upload into the system. However, in the later versions, it is expected that such data will be auto fed into the UDI platform through API calls. In such cases, the bulk data upload will need to be checked on a line by line basis for the validity of each of its fields. URN generated in such cases, will be stored in the CBS and where required may need to be passed on to the original channels also. Appropriate functions for the same to be built in.

12.3 Aadhaar Vault

Design and implement digital Aadhaar Vault for storing Aadhar numbers of policyholders alongside UDI repository in compliance with directions issued by UIDAI.

It is expected that most of the banks have a Aadhar vault solution built in. However, the UDI platform would also require an Aadhaar vault to be implemented

Digital Vault also referred as Aadhaar Vault for Aadhaar storage solutions for storing of Aadhaar Numbers and any connected Aadhaar data on separate secure database/vault/system is needed. Aadhaar Data Vault is a centralized storage for all the Aadhaar numbers collected by AUA's (Authentication User Agency) /KUAs (KYC User Agency) for specific purposes under Aadhaar Act and Regulations, 2016. It is a secure system inside the UDI infrastructure accessible only on need to know basis.

1. Aadhaar number has been identified as “Identity Information" under the Aadhaar Act 2016 and can uniquely identify residents in India. Aadhaar Data Vault is designed to reduce the footprint of Aadhaar numbers within the systems/environment of the organization by storing in centralized secured database.
2. Each Aadhaar number is to be referred by an additional key called as Reference key, which is to be generated through the proposed solution which cannot be reverse traced. Mapping of the reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault. The reference key generated for the Aadhaar number is to be used in the UDI for control of duplicate enrolments, duplicate claims and for fraud control. As per UIDAI guidelines, UID token id should be placed in Aadhaar vault.
3. The Bidder is required to Supply required Hardware and Software with redundancy, HSMs with required licenses, FM support, install & deploy the solution.
4. The reporting and logging system of the Aadhaar Data Vault shall integrate seamlessly with existing SIEM Solution.
5. The bidder is required to maintain the RTO and RPO as per the UDI requirements.
6. The Hardware / OS required and the encryption hardware i.e. HSM should be provided by the bidder.
7. The bidder should ensure the availability of spare parts during contract period.
8. The Bidder should comply with UIDAI, DFS and ASA/KSA guidelines specified by UIDAI/NPCI for the proposed solution. HSM should have capability of Key rotation and handle the scalability for High availability.
9. UID Token, encrypted Ekyc-XML data ,hashed UID, and any relevant demographic data and/or photo of the Aadhaar Number should be stored in the Aadhaar Data vault.
10. Only trusted communications must be permitted in and out of the vault. This should be done via secured API/Micro-service dedicated to get the mapping and controlling access to the API/Micro-service at application level. Any authorized users needing to access this mapping must go via applications allowing them to view/access this data with appropriate user authentication, controls and logging. (user access for proposed system should be compatible with the PIM solution)
11. The Aadhaar Data Vault must implement strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access as well as it should be auditable.
12. The Aadhaar Data Vault should support mechanisms for secure deletion/ updation of Aadhaar number and corresponding data if any as required by the data retention policy of the entities
13. Bidder should adhere all the guidelines, Regulations, Circulars, FAQ etc. by UIDAI or any other regulator within time lines.
14. Bidder should support audit of Aadhaar Data vault systems, API, interfaces, logs etc. and should comply with auditor observations.

15. All modifications/ enhance3ments as per revised guidelines of UIDAI or any other Authority will be carried out as within scope of the project, before GoLive of the project.

12.4 Correction Module:

Correction/changes to the data received will be made only with the multiple approvals of the entity involved and the project team of the UDI.

- Correction of data in the main repository - the update to be made only to the status of the data row and not the actual datapoint, to accommodate fresh entry of data. Any change/correction will be done only after due authorization from the entity and UDI Project manager.
- Correction of data in the company data store before entry into the main repository
- System driven changes – to be added to the tool. Transparent and traceable system needed.
- Deletion of data when an error is noticed. This will be a soft delete and audited.

All work on the database to be carried out only on the cloud. At no point, should the data be available in the individual devices (desktop, laptop, mobile, etc) of the solution provider.

The correction module should carry forward corrections, if any to all the related modules and entries.

13 Data Audit

Vulnerability Assessment Penetration Testing (VAPT) to be conducted quarterly or as specified by the regulatory authority/ UDI is also part of the scope of the CERT-IN empaneled testing agency.

Information Security Audit to be conducted quarterly or as specified by the regulatory authority/ UDI is also part of the scope of the CERT-IN empaneled testing agency. However, the bidder has to ensure that the IS Audit is conducted before the Go-Live and all observations are closed.

The Bidder should setup the UAT environment for testing of the solution before implementation of the solution in the production environment. The UAT setup shall be used for the customization of any changes before movement in production. The setup would be kept available at all times during the contract period.

Bidder team will test and coordinate the testing of the application by the various stakeholders and will be responsible for performing the below activities:

1. Development of suitable testing methodology/testing strategy document
2. Development of test cases based on the phase and enhancements incorporated within the system.

3. Maintain a track of errors, bugs and customization requests and their resolutions.
4. Testing must include test cases on calculation and application of charges, EOD / BOD, premium calculation, batch job execution, month end / half year end and yearly EOD / BOD, Claim generation response time etc.
5. Acceptance testing shall broadly cover the testing of functionalities, migrated data (pre and post migration), and all interfaces to verify that the proposed solution conforms to the business & technical requirements and Gap analysis Report, Bandwidth and response time.
6. Bidder must fix the bugs, carry out necessary rectifications and deliver patches/version towards changes which would be reported by the UDI users.
7. Bidder/ 3rd party testing agency is required to factor in devices and all other required devices of various form factors for testing of solution.
8. UDI shall accept the application software only after critical or major bugs are fixed and are ready for production Implementation.

Data Audit

Bidder has to carry out Data Audit based on the recommended audit methodology.
The Bidder shall perform the following audit checks:
Data integrity checks: Pre-migration and post-migration data sets should be compared for data integrity issues. Data integrity checks should check the following data parameters:

1. Raw data integrity
2. Business rules
3. Log Tables
4. Configuration/ Parameterization table

Deliverables of data audit

1. Data migration audit strategy.
2. Migration process review report
3. Field wise Exceptions reports (pre & post)
4. Final compliance report, post migration.

14 Disaster Recovery

To manage the Disaster Recovery Operations more efficiently, the project envisages an Automated DR solution.

The Bidder is required to design, supply, install, train, customize, test, implement, rollout and maintain the ADR solution and hardware at the DC and DR as per the requirements of this RFP. The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases.

The Bidder is expected to provide and implement an ADR solution encompassing the following functions:

1. Align the DR Management to meet the client's business objectives.
2. Provide an efficient, rationalized and integrated Automated DR solution.
3. Maintain the desired RPO and RTO for applications and IT Infrastructure
4. Continuously improve efficiency of DR Drill.

The Disaster Recovery Management Solution should be a single integrated business solution covering all functionality and flexibility required to carry out the Disaster Recovery operations in the current and foreseeable future. It should support all kinds of monitoring that are involved in a DR environment and also should be able to perform DR Drills in a complex environment. It should be a ready to deploy solution with pre-defined templates, and not merely a framework, to support a green field operation. It should provide a competitive edge to the project, especially with respect to offering innovative products with a quick time to operational efficiency, operational controls, superior service delivery, better risk management, higher experts retention, highest levels of regulatory and internal policy compliance and timely management information to support quick decision making at all levels of the process chain. The contracting party is looking out for a comprehensive DR Management Solution for its Core Insurance Applications, UDI web based platform.

The high-level scope of work for the bidder is to provide the following services:

1. Design, size, supply, implement and maintain the automated DR solution including hardware, OS, database etc.
2. At least first 4 DR drills to be conducted by OEM after successful implementation of proposed solution and training to be given to the stakeholders. Subsequently, all DR drill to be performed by bidder.
3. Any change management process or upgrade process in software should not affect the production database or application. No changes should be prescribed in the database or replication.
4. The offered solution shall have workflow-based monitoring, management, troubleshooting features.
5. The offered solution should have reporting capability for the real time monitoring of a DR solution parameter like RPO (at DB level), RTO, and replication status and should provide alerts (including SMS and e-mail alerts) on any deviations.
6. The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms.
7. The proposed solution must have pre-packaged support for all widely used databases like Oracle, MSSQL, MYSQL, Sybase, PostGre SQL, DB2, NoSQL, etc. It must support both physical and virtual platforms.
8. The proposed solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters.
9. The offered solution should integrate with AAA (Authentication, Authorization and Accounting) systems like Active Directory / LDAP or equivalent.

10. The offered solution Solutions should be compatible with database log-based replication and transaction-based replication.

14.1 DR Setup

A solution that can take care of downtimes is acceptable if the same handles the features and requirements listed below:

- All Application, Database, Stateless and IT infrastructure servers are replicated to DR site and are operational at all the time.
- Bidder should make necessary setup to enable the DR within the agreed timelines.
- Bidder should carry out the deployment of the application in DC and DR, UAT as applicable.
- To ensure proper rollback, bidder has to ensure that the old setup at all the locations is As –IS as per the agreed timelines during migration strategy formulation.
- DC and DR to be on cloud
- To achieve complete replication of data and maintaining one copy of data on DR site, the storage shall be replicated 100% and shall be sized accordingly to maintain the data at DR.
- Network components and management is within scope
- Security provisions should take care of DC and DR
- DR Site would be Hot or warm Disaster recovery Site. DR resources are configured at 100% of Production Data Centre capacity.
- Recovery point operation is High/Aggressive (near zero to Minimal data loss)
- Recovery time operations to be near zero using Multi-Cloud Global Server Load Balancing (GSLB)

The bidder is required to provide IT service continuity and disaster recovery services for UDI production environments and their associated infrastructure. The bidder must demonstrate that it will consistently meet or exceed UDI business continuity and disaster recovery requirements.

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines

1. Maintain and update Business Continuity plan.
2. Maintain and update disaster recovery plan
3. Ensure successful replication between production and DR
4. Notifying UDI promptly if a Disaster recovery scenario/condition arises
5. Assisting UDI in execution of DR plan in such scenario
6. Perform periodic recovery testing
7. Developing and executing test plans as per defined periodicity or as and when required
8. Documentation for Business continuity plan, Business continuity strategy plan & Roles and responsibility matrix for DC and DR team
9. Coordinate involvement of users for DR testing
10. Track and report DR test results

11. Develop an action plan and timeline to address DR testing results
12. Implement DR action plans and provide ongoing status reporting until completion of all action items
13. Initiate the DR plan for UDI in the event of an UDI declared DR situation per UDI Disaster Recovery policies and procedures.
14. Perform quarterly DR drills or DR drills based on UDI's periodicity
15. Coordinate with UDI and third parties during a DR situation per UDI Disaster Recovery policies and procedures

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines. After implementation of the supplied hardware and software, bidder need to perform the first DC DR Drill in totality within one month of Go-Live.

14.2 IT service continuity

The bidder is required to provide IT service continuity and disaster recovery services for UDI production environments and their associated infrastructure. The bidder must demonstrate that it will consistently meet or exceed UDI business continuity and disaster recovery requirements.

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines

a. Maintain and update business continuity plan.
b. Maintain and update disaster recovery plan
c. Ensure successful replication between production and DR
d. Notifying contracting party promptly if a disaster recovery scenario/condition arises
e. Assisting contracting party in execution of DR plan in such scenario
f. Perform periodic recovery testing
g. Developing and executing test plans as per defined periodicity or as and when required
h. Documentation for Business continuity plan, Business continuity strategy plan & Roles and responsibility matrix for DC and DR team
i. Coordinate involvement of users for DR testing
j. Track and report DR test results
k. Develop an action plan and timeline to address DR testing results
l. Implement DR action plans and provide ongoing status reporting until completion of all action items
m. Initiate the DR plan for UDI in the event of a contracting party declared DR situation as per UDI Disaster Recovery policies and procedures.
n. Perform quarterly DR drills or DR drills as suggested by contracting party
o. Coordinate with contracting party and other third parties during a DR situation as per UDI Disaster Recovery policies and procedures

14.3 DC -DR Drills

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with UDI's requirements and any statutory or regulatory guidelines. After implementation of the supplied hardware and software bidder need to perform the first DC DR drill in totality within one month in coordination will all other vendors of the UDI through ADR solution.

1. Bidder need to perform minimum of 4 DC-DR drill in each year during the contract period as per the discretion of the contracting party.
2. All the DR Drills needs to be done from the supplied ADR tool
3. Bidder needs to allocate adequate resources, do project management and work closely with the application owner for performing the DC-DR Drills whenever planned by the contracting party.
4. Any configuration level changes which can impact the DC-DR drill need to be informed to ADR team before handover to avoid issues during the drill.
5. During DC-DR drill bidder need to allocate appropriate resources onsite to avoid any failure and delays which will be penalized appropriately
6. Bidder needs to perform project management and all reporting and pre and post environment preparation to avoid any failure in the drill.
7. Maintain and update business Continuity plan
8. Maintain and update disaster recovery plan
9. Ensure successful replication between production and DR
10. Notifying contracting party promptly if a Disaster recovery scenario/condition arises
11. Assisting contracting party in execution of DR plan in such scenario
12. Perform periodic recovery testing
13. Developing and executing test plans as per defined periodicity or as and when required
14. Documentation for business continuity plan, Business continuity strategy plan & roles and responsibility matrix for DC and DR team
15. Coordinate with all the users involved in DR testing
16. Track and report DR test results.
17. Develop an action plan and timeline to address DR testing results.
18. Implement DR action plans and provide ongoing status reporting until completion of all action items.
19. Initiate the DR plan for UDI in the event of contracting party declared DR situation as per their Disaster Recovery policies and procedures.
20. Perform quarterly DC-DR drills as suggested by contracting party
21. Coordinate with contracting party and other third parties during a DR situation as per UDI Disaster Recovery policies and procedures.
22. Contracting party can also do an unplanned DC-DR drill which bidder needs to support and design the system accordingly.

14.4 RTO / RPO Management

The bidder needs to maintain the below RTO and RPO parameters of the all the in-scope equipment's and software as mentioned below:

Application Name	RTO / RPO
UDI web-based platform & app	RTO: - 4 hours RPO: - 60 minutes

Replication

1. Monitor the RTO and RPO of complete solution as per the contracting party
2. Monitor and manage the replication between the DC and the DR
3. Generate reports to review the performance of the replication
4. Ensuring the RTO and RPO are maintained of the complete solution as per the contracting party

15 Management Services: Helpdesk Support

All stakeholders would require help in entering and using the platform. In addition to training, technical support in connecting through APIs, usage of the system, handling technical and connectivity issues, performance issues, etc. would be necessary.

Grievances will be entered into UDI through an interface by the banks or by the client through interlinked portals. These grievances are sent to the banks/ insurance companies are necessary action. Thereafter, the same is followed up until the closure status is not updated on the portal against each case.

Suitable reports and lists of the grievances and their solutions can be extracted for follow-up and analysis purposes.

To this end, a helpdesk support would be required for handling both the issues and support needed by the stakeholders in managing and using the UDI as well as to handle complaints once the system goes live.

An indicative list of the helpdesk activities shall include the following minimum activities:

- Customer care call handling and email handling (this would include issue resolution on call)
- Daily reporting of calls received.
- Tracking of issues identified and monitoring them till their closure
- Co-ordination with UDI and system support team on issue reporting
- Generation of daily payment reconciliation report and providing it to concerned UDI official for approval/ further action.
- Managing the updation of master data in the UDI web-based platform (Office master updation, Employee Master updation)
- Monthly analysis of UDI web-based platform trends

- Daily MIS reporting to UDI
- Helpdesk requests for extending technical support on UDI web-based platform functionalities
- Deployment of web-based tool for the helpdesk
- Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through a dedicated phone number
- Track each incident / call to resolution
- Escalate the calls, to the appropriate levels, if, necessary as per the escalation matrix agreed upon and developed by Bidder and UDI
- Analyse the incident / call statistics and provide monthly reports including but not limited to: Type of incidents / calls logged/ resolved
- Update the frequently asked questions on Web UDI web-based platform to assist end users in resolving basic issues themselves

16 WARRANTY & ON-SITE MAINTENANCE

Hardware / Software Acceptance: Contracting party will carry out the acceptance tests for testing of software, hardware and verification that the supplied components are as per bill of material through contracting party and the PMO resources provided Team. The Bidder shall assist contracting party in all acceptance tests to be carried out by contracting party. Bidder needs to rectify all the gaps highlighted in the Acceptance testing without any additional cost to contracting party

Hardware / Software Go-Live: The respective hardware and software will be termed as Go-live only when the application for which the hardware is allocated goes in production and all the data is migrated.

The Bidder shall undertake to provide an onsite comprehensive 3 (three) Year Warranty from the date of Go-live and acceptance of Hardware and AMC for next 2 (two) years (BACK-TO-BACK with OEM) for all supplied Hardware commencing from the date of commissioning at the respective delivered locations of the Company as provided in the Purchase Order / Contract for Supply.

Replacement under warranty clause shall be made by the Supplier free of all charges at site including freight, insurance and other incidental charges.

The Bidder shall undertake to provide an onsite comprehensive 1 (One) Year Warranty and ATS for next 4 (four) years (BACK-TO-BACK with OEM) for all supplied Software commencing from the date of Go-Live and sign off by UDI of the software for the respective delivered locations of the Company as provided in the Purchase Order / Contract for Supply.

The Bidder will be single point of contact and responsible for AMC, ATS, guarantees & warrantees for all components, hardware, software, etc. Bidder to note:

a. Warranties pertaining to Software / Applications, other Peripherals starts post Installation of the license at Production with the period of warranty as one year. ATS for Software/ Application shall begin post Completion of Warranty.

b. During FM period, Bidder will be responsible for:

   i. Overall maintenance and working of the Solution
   ii. Bug fixing and delivery of patches/ version changes effected
   iii. Creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc. of Application software, etc.
   iv. Provision should be available for version control and restoring the old versions if required by contracting party
   v. Enhancement, modifications, customization, patches, upgrades due to statutory, regulatory, industry, changes till the SRS Sign off will be provided at no additional cost to contracting party. During FM period, if due to any statuary and regulatory requirement, system requires any enhancement due to which there is major impact on sizing, then required procurement and delivery of hardware and software will be on mutually agreed terms and conditions. However, bidder has to provide all the services on CR basis to contracting party.
   vi. Configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, replacement/ support, technical support for application and data maintenance, recovery, query generation and management etc. of all software supplied under this RFP document.
   vii. Bug fixing should be undertaken in the event of software failure causing an interruption of operation of the proposed applications as per the response/ resolution times defined by contracting party.
   viii. All the detected software errors must be notified and corrected, as per the agreed timelines
   ix. Provide contracting party with monthly hardware utilization/performance monitoring reports and alert contracting party in case of any performance issues by suggesting future capacity planning.
   x. The operational support staff should have support experience for UDI web-based platform and app.
   xi. Conduct DR drills in conjunction with the UDI's requirement/procedures

c. Software/ Applications Delivery must coincide with cloud deployment.

Bidder has to deploy competent resources for the team to provide necessary maintenance and support as per the requirements of UDI. Bidder has to deploy adequate resources to ensure that the systems are up, and customer services are not impacted. To ensure that the SLAs are met, the Bidder, if required, will need to deploy additional resources during the contract period including implementation schedule without any additional cost to contracting party.

Bidder has to also ensure availability of resources spanning across all parts of implementation including Project Preparation, Solution Design, Configuration & Customization, Integration, UAT and Training.

The successful bidder shall not change any member of the project team during the course of the project without written consent from contracting party.

17 Terms & Conditions

17.1 General

17.1.1 Definitions

All hardware (required for interface, staging, Web Server, development and training server, and related hardware components) and system software components required for the project, must be included in the bill of material of the bidder. In case, bidder fails to do so, and the project demands additional components at a later stage, then bidder will have to provide additional components at no additional cost to the contracting party.

17.1.2 Amendment bid document:

At any time prior to the deadline for submission of bids, contracting party may for any reason either on its own initiative or in response to a clarification requested by a prospective bidder, modify the bid document, by amendment. All prospective bidders that have received the bid document will be notified of the amendment. The same will be binding on them. In order to allow prospective bidders reasonable time in which to take the amendment in to account in preparing their bids, contracting party may, at its discretion, extend the deadline for a reasonable period for the submission of bids. Details will be communicated and published accordingly.

- Contracting party also reserves the right to change any terms and conditions of the RFP and its subsequent addendums as it deems necessary at its sole discretion. Contracting party will inform the bidder about changes, if any before the deadline of bids submission.
- Contracting party may revise any part of the RFP, by providing an addendum to the bidder at stage till commercial bids are opened. Contracting party reserves the right to issue revisions to this RFP at any time before the deadline for bid submissions.
- Contracting party reserves the right to extend the dates for submission of responses to this document.
- Bidder shall have the opportunity to clarify doubts pertaining to the RFP in order to clarify any issues they may have, prior to finalizing their responses. A detailed pre bid meeting would be held to address any questions. Responses to inquiries and any other corrections and amendments will be distributed to the bidder in electronic mail format.
- **Preliminary Scrutiny** – Contracting party will scrutinize the offer to determine whether

it is complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. Contracting party may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on the Bidder and Contracting party reserves the right for such waivers and its decision in the matter will be final.

- **Clarification of Offer –** To assist in the scrutiny, evaluation and comparison of offer, contracting party may, at its discretion, ask the Bidder for clarification of their offer. Contracting party has the right to disqualify the Bidder whose clarification is found not suitable to the proposed project.
- Contracting party reserves the right to make any changes in the terms and conditions of purchase. Contracting party will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations.
- **Erasures or Alterations –** The offer containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "as given in brochure / manual" is not acceptable. Contracting party may treat the offers not adhering to these guidelines as unacceptable.
- **Right to Alter Quantities –** Contracting party reserves the right to alter the requirements specified in the tender. Contracting party also reserves the right to alter/ modify any/some/all of the requirements, as it may deem necessary, and notify the same through mail before the last date for submission of response under this RFP. The bidders should be agreeable for the same. The bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by Contracting party for alteration in quantities. Bidder agrees that there is no limit on the quantities that can be altered under this contract. During the contract period the bidder agrees to pass on the benefit of reduction in pricing for any additional items to be procured by Contracting party in the event the market prices / rate offered by the bidder are lower than what has been quoted by the bidder as the part of commercial offer. Any price benefit in the products, licenses, software, services& equipment should be passed on to Contracting party within the contract period.

17.1.3 Sub-contracts

As per scope of the RFP, subcontracting is explicitly prohibited. The Bidder shall provide the software and other support and maintenance services by itself. Contracting party would have a single agreement with the shortlisted Bidder. Subject to other terms and conditions of this RFP, If the Bidder is doing any tie-up with any other Service Provider's for taking its support then same shall be only an internal arrangement between bidder and such Service Provider but Contracting party neither endorse such action of availing the Service Provider's services

nor the bidder can relieve itself from the obligations and duties under the Agreement. The bidder is solely and entirely responsible to Contracting party to provide the solutions, services and all support as per this RFP, details should be submitted along with the bid response and purpose of tie-up. Bidder will not be allowed to change the vendors at later stage. Subcontracting shall be permitted for data entry only, if required at the sole discretion of the Contracting party.

In case of Bidder availing services of any service provider for data entry, the bidder is responsible for all the services provided to the Contracting party regardless of which entity is conducting the operations. The Bidder is also responsible for ensuring that the sub-contractor comply with all security and privacy requirements of the contract and Contracting party can obtain independent audit report for the same

The Bidder is required to provide the solutions, help and support by itself/himself. If the bidder so request, whether or not to allow subcontracting and if so to whom same will be allowed shall be at the sole discretion of Contracting party which has to be with prior consent of Contracting party and decision of Contracting party whether or not to allow subcontracting and if allowed to whom it will be allowed is final and binding on bidder. Whether it is termed as subcontracting or service provider, it shall be understood that the same is pure service provider with the Bidder solely responsible and liable to provide the Solutions to Contracting party.

17.1.4 Conditional bids

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

17.1.5 Performance Security

Within 15 days after the receipt of notification of award from Contracting party, the bidder shall furnish performance security to Contracting party, which shall be equal to 3 percent (3%) of the value of the contract - valid till date of expiry of three-year Contract period in the form of a bank guarantee from a nationalized/ scheduled bank as per the norms laid by the RBI.

Failure by bidder to submit the Performance security will result in invocation of Bid security held by the Contracting party.

17.1.6 Installation and Implementation

All professional services necessary to successfully implement the proposed solution will be part of the RFP. These services include, but are not limited to, Project Management, Training, Deployment methodologies etc.

The Bidder should submit as part of technical Bid an overview of Project Management approach of the proposed solution

Bidder should ensure the quality of methodologies for delivering the services and its adherence to quality standard.

Bidder should be willing to transfer skills to relevant personnel by means of training and documentation.

Bidder should provide and implement patches / upgrades / updates for Software / OS / Middleware etc. as and when release by the Bidder or as per requirements of the UDI. Bidder should bring to notice of the contracting party all release /version change on timely basis.

Bidder should obtain a written permission from the contracting party before applying any of the patches / upgrades / updates.

In case contracting party chooses not to upgrade the software/ OS/ Middleware version, Bidder should able to support the available version of UDI till the end of application support period of 5 years.

All product updates, upgrades & patches should be provided by the Bidder free of cost during warranty and ATS period.

Bidder should provide legally valid software solution. The detail information on license count and type of licenses should also be provided to the contracting party.

For every change request Bidder should provide detail effort estimates to the contracting party including the code change requirements, affected applications, resource requirements, testing requirement, time required to implement the changes etc.

Bidder should provide latest version for all the solution components

17.1.7 Delay in Bidder's performance

Implementation of the Solution and performance of service shall be made by the bidder in accordance with the time schedule specified by contracting party.

Any unexcused delay by the bidder in the performance of his implementation/service/other obligations shall render the bidder liable to any or all of the following sanctions: for feature of his performance security, imposition of liquidated damages, and/or termination of the contract for default.

If at any time during performance of the contract, the bidder should counter conditions impeding timely implementation of the Solution and/or performance of services, the bidder shall promptly notify contracting party in writing of the fact of delay, its likely duration and cause(s), before the scheduled delivery/installation /implementation date. contracting party shall evaluate the situation after receipt of the bidder's notice and may at their discretion extend the bidder's time for delivery/installation/implementation, in which case the extension

shall be ratified by the parties by amendment of the contract. If the bidder's request to delay the implementation of the Solution and performance of services is not found acceptable to contracting party, the above mentioned clause would be invoked.

Delivery of the solution and performance of the services shall be made by the Bidder in accordance with the time schedule, technical specification, scope of the project and other terms & conditions as specified in the RFP/SLA/Contract. Any delay in performing the obligation /defect in performance by the bidder may result in imposition of liquidated damages, invocation of Performance Bank Guarantee and/or termination of contract.

17.1.8 Payment terms

The bidder must accept the payment terms proposed by contracting party. The financial bid submitted by the Bidder must be in conformity with the payment terms proposed by contracting party. Any deviation from the proposed payment term should not be accepted. contracting party shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of contracting party.

Hardware, Software and other components to be provided for execution of project should be sized for entire contract period by considering Scope, functional & technical requirements and SLAs.

However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit as defined in the RFP, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by UDI Technical committee. The Bidder must accept the payment terms proposed by contracting party as proposed in this Section. The financial offer submitted by the Bidder must be in conformity with the payment terms proposed by contracting party. Any deviation from the proposed payment terms would not be accepted.

17.1.9 Penalties and delays in Bidder's performance

In case the vendor fails to meet the SLA mentioned for various components, penalty will be imposed as per the terms of the agreed Service Level Agreement.

17.1.10 Currency of Payments

Payment shall be made in Indian Rupees (INR)only.

17.2 Other RFP Requirements

The project office of contracting party is floating this RFP. However, the Bidder getting the contract shall install and commission the solution, procured through this RFP, at UDI's DC and

DR or at such centers as contracting party may deem fit and the changes, if any, in the locations will be intimated to the Bidder.

Technical Inspection and Performance Evaluation - Contracting party may choose to carry out a technical inspection/audit and performance evaluation of products offered by the Bidder. The Bidder would permit contracting party or any person / persons appointed by contracting party to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (performing the benchmark, travel, stay, etc.) incurred for the same would be borne by the Bidder and under no circumstances the same would be reimbursed to the Bidder by contracting party.

OEM's Authorization Form – The Bidder should furnish a letter from original equipment manufacturer for each component

Making contracting party aware about latest developments in the sector would enable adopting the right set of tools, policies and procedures while deploying their application and handling seamless operation.

UDI application should always be compliant to law of land and amendment in rules and regulations hereunder.

17.2.1 Cloud Deployments

The Cloud Computing services would fall under the legal ambits of following legislations: Guidelines for Enablement of UDIs for Adoption of Cloud Management

- 'Cloud services' are recognized under the Integrated Goods and Services Tax Act 2017 (the GST Act) under 'online information and database access or retrieval services' and therefore the services rendered by Cloud Services Providers would be subject to GST.
- Information Technology Act Section 43 A and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 (the Privacy Rules) under Information Technology Act provide guidelines for collection, use and protection of the sensitive personal data or information of persons by a body corporate that possesses, deals with or handles such data.
- The IT Act and the Privacy Rules together set out the regulatory framework for creation, collection, storage, processing and use of electronic data (including personal and sensitive personal information recorded in electronic form) in India.
- CSP's in India would also need to follow the principles of the Information Technology (Intermediaries Guidelines) Rules 2011 and (Intermediary Guidelines) under the Information Technology Act.
- Government of India has drafted a Personal Data Protection Bill and the same once notified will overhaul the existing framework of privacy and data protection regime in India. General Data Protection Regulation, EU and it, inter alia, enhances the stringency of obligations and corresponding penalties governing data protection from a customer

perspective.

- In addition to the IT Act and Privacy Rules, the use of Cloud Computing in the banking and insurance sectors is subject to specific restrictions. The RBI's guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks read along with the Report of Working Group of RBI on Electronic Banking set out specific requirements to be complied with by banks while engaging Cloud Service Providers. These requirements, inter alia, relate to vendor selection, data security, form of agreement, business continuity and disaster recovery or management practices.
- The Insurance Regulatory and Development Authority of India's (IRDAI) Guidelines on Information and Cyber Security for Insurers require insurers to comply with requirements, inter alia, in relation to data, application and network security, incident management, and information security audit while using services from a Cloud Service Provider, also the Web application hosted on the cloud has to comply ISNP and ISMS standards or any other regulation proposed in future
- The government retains the authority to intercept any information transmitted through a computer system, network, database or software for the prevention of serious crimes or under grave circumstances affecting public order and national security. The Ministry of Home Affairs has passed an order "authorizing" ten central agencies under Section 69(1) of IT Act, 2008, read with Rule 4 of IT Rules, 2009, for the "……purposes of interception, monitoring Guidelines for Enablement of UDIs for Adoption of Cloud Management Office Page 96 of 99 and decryption of any information generated, transmitted, received or stored in any computer resource…"

17.2.2 Solution with Infrastructure as a Service (IaaS):

The CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including compute, operating systems, storage, network, security, etc.

The indicative list of responsibilities of CSP for IaaS Cloud Service Model is as follows:

- Provide Compute, Storage, hypervisors, network interfaces and other fundamental compute resources
- Provide redundancy and high availability for the IT infrastructure (IT Hardware – compute, network, storage, security) to meet the guidelines and SLA terms as laid down by MeitY.
- Provide auto-scalable, redundant and dynamic computing capabilities for virtual machines created as a part of the provisioned infrastructure. Provide interoperability support with regards to available APIs, data portability etc. Provide self-service tools to the UDIs that can be used to manage their Cloud infrastructure environments
- Network Port Connectivity: Ensure network port connectivity for links between the UDI location(s)/Infrastructure and other Cloud environments (DC/DR)

- Tools: Provide relevant tools and services for backup, migration and replication of data, application and associated Databases
- Security: Ensure appropriate physical and logical security controls for Cloud deployment and service models as envisaged by MeitY
- Patch Management: Upgrade, maintain and deploy patches for underlying infrastructure and related components on cloud
- Disaster Recovery: Offer DR Services meeting DR requirements of the UDI in consonance to the guidelines laid down by MeitY
- Cloud Access Logs: Provide authorized access to logs of all user activity within an account and the recorded information including API details, etc.
- Data Privacy: To ensure data privacy guidelines as defined by MeitY or contracting party or Government of India are met by the CSP/MSP as applicable during the migration and other Cloud related activities
- Exit Management: To provide support to the contracting party in case of Cloud to Cloud migration, for transferring data & applications, its associated databases, at the time of exit management and in line with the guidelines defined by MeitY.
- Compliances: To ensure all the compliances as defined by MeitY for empanelment of Cloud Services offered by CSP and the security guidelines as defined by STQC.
- Audit Support: Provide support during Audit by STQC / MeitY empaneled agency or any agency appointed by the contracting party.

17.2.3 Role of Bidder

This section lists down the indicative responsibilities of Bidder whose services are being procured by the bidder. The responsibilities specific to a Bidder include but not limited to are specified as below: -

- Requirement Gathering: Gathering requirements, including business, system and functional, from the UDIs
- Requirement Mapping: Map key functional and non-functional requirements with the optimal solutions offered by the CSP
- Design & Develop application(s) / software(s) to meet UDI needs / requirements
- Capacity Sizing: Conduct Capacity Sizing and planning for applications
- Application Lifecycle management
- Integration Services: for applications as per the requirement
- Test Plans: Executing Test plans to test application functionality
- Service Change Requests raised by the contracting party
- Patch Management: Upgradation/patching application, database and maintenance

- Support Services: Providing application support in case of any technical error or glitch
- Any other requirement as specified by the contracting party
- Release Management by performing functional testing, performance testing, to provide well documented development & testing process artifacts,
- Documentation: Business Requirements Document (BRD) , Functional Requirement Specifications (FRS),Software Requirement Specifications (SRS) ,Software Design Documents (including HLD, LLD etc.) , Requirements Traceability Matrices (RTM) , Test Plan, Test Cases & Test Reports ,Code Review Reports, Database Review Reports, Project Implementation Plan, User Manual, Deployment Guide.
- To provision convenient migration policies, for switching to alternative PaaS/IaaS provider to prevent vendor lock in the Managed Service Provider/SI must provide managed services for various components on the cloud as per the scope of work finalized and the MSP must share relevant reports periodically as per the scope of work signed off between UDI and the MSP/SI.

17.2.4 Testing requirements

In addition to the software testing of functionality, the following testing to ensure robust and responsive hardware and infrastructure are recommended

i. Infrastructure testing - various testing procedures including infrastructure (server, storage and network infrastructure) provided on Cloud.
ii. VM testing
iii. Storage/Disk IO testing.
iv. Network throughput and latency testing
v. CPU and RAM benchmarking testing
vi. Read/Write latency testing
vii. Data Replication Testing
viii. Firewall policy and configuration testing
    a. Data Integrity Testing
    b. Reverse Replication Testing
    c. Switch over testing

17.2.5 Patent Rights

For any licensed software used by the Bidder for performing services or developing software for the UDI, the Bidder should have right as well right to license for the outsourced services or third-party software development. Any license or IPR violation on the part of Bidder should not put the contracting party at risk. Contracting party should reserve the right to audit the license usage of the Bidder.

The Bidder shall, at their own expenses, defend and indemnify contracting party against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad. In case of violation/ infringement of patent/ trademark/ copyright/ trade secrete or industrial design, the bidder shall after due inspection and testing get the solution redesigned for contracting party at no extra cost.

18 Terms of Reference ('ToR')

18.1 Contract Commitment

Contracting party intends that the contract, which is contemplated herein with the Bidder, shall be for a period of three years (Extendable on mutually agreed terms and conditions).

18.2 Ownership, Grant and Delivery

The contracting party shall own the assets/components including but not limited to equipment, software, licenses, processes, Documents, etc., supplied by the Bidder arising out of or in connection with this Contract.

However, all the risk and liability arising out of or in connection with the usage of the equipment, assets/components during the term of the Contract shall be borne by the bidder.

The Bidder must transfer all goods, clear and unencumbered titles to the assets and goods procured for the purpose of the Project to the Contracting party at the time of delivery of assets and goods. This includes all licenses, titles, source code, certificates, hardware, devices, equipment's etc. related to the system designed, developed, installed and maintained by the Bidder.

The contracting party reserves the right to use the excess capacity of the licenses supplied by the Bidder for any internal use of UDI application or its affiliates, or subsidiaries at no additional cost other than the prices mentioned in the commercial bid. The Bidder agrees that they do not have any reservations on such use and will not have any claim whatsoever against such use of the hardware, licenses and infrastructure.

Further the Bidder also agrees that such use will not infringe or violate any license or other requirements.

18.3 Completeness of Project

The project will be deemed as incomplete if the desired objectives of the project under Scope of Work of this document are not achieved. The completeness of the project is subject to the stakeholder users testing and using the application to its capability and at least 5 each of the banks and insurer end users satisfactorily consuming the services provided. The satisfaction is under the sole discretion of the contracting party, and is dependent on timely and successful completion of the project, and handling all service related queries/problems during the course of operation.

18.4 Assignment

Contracting party may assign the Services provided therein by the Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. Contracting party shall have the right to assign such portion of the services to any of the sub-contractors, at its sole option, upon the occurrence of the following:

(i) Bidder refuses to perform;

(ii) Bidder is unable to perform;

(iii) termination of the contract with the Bidder for any reason whatsoever;

(iv) Expiry of the contract. Such right shall be without prejudice to the rights and remedies, which contracting party may have against the Bidder. The Bidder shall ensure that the said subcontractors shall agree to provide such services for UDI application at no less favorable terms than that provided by the Bidder and shall include appropriate wordings to this effect in the agreement entered into by the Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of the Bidder to perform or termination/expiry of the contract.

18.5 Canvassing/Contacting

Any effort by a Bidder to influence the Company in its decisions on Bid evaluation, Bid comparison or award of contract may result in the rejection of the Bidder's Bid. No Bidder shall contact the Company on any matter relating to its Bid, from the time of opening of Commercial Bid to the time the Contract is awarded.

18.6 Indemnity

The Bidder shall indemnify the Contracting party from and against all Third Party claims of infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied Software/hardware/manpower etc. and related services or any part thereof. Contracting party/user department stands indemnified from any claims that the hired manpower / Bidder's manpower may opt to have towards the discharge of their duties in the fulfilment of the work orders. Contracting party / user department also stands indemnified from any compensation arising out of accidental loss of life or injury sustained by the hired manpower / Bidder's manpower while discharging their duty towards fulfilment of the work orders. Contracting party shall provide bidder with prompt notice of such claim and allow Bidder to control the defence of such claim. Indemnity shall be limited to damages that may be finally awarded against the bidder.

The Bidder shall not indemnify contracting party for -

(i) Any loss of profits, revenue, contracts or anticipated savings or

(ii) Any consequential or indirect loss or damage however caused

18.7 Inspection of Records

Technical Representative of the Contracting party or Contracting parties reserves the right to inspect and monitor/assess the progress/performance/maintenance of the bidder at any time during the course of the Contract, after providing due notice to the Bidder. The Contracting party may demand and upon such demand being made, the contracting party shall be provided with any document, data, material or any other information which it may require, to enable it to assess the progress of the Project.

Technical Representative of the Contracting party or Contracting parties shall also have the right to conduct, either itself or through an independent audit firm appointed by the Contracting party as it may deem fit, an audit to monitor the performance by the Bidder of its obligations/functions in accordance with the standards committed to or required by the Contracting party and the Bidder undertakes to cooperate with and provide to the Contracting party / any other Bidder appointed by the Contracting party, all documents and other details as may be required by them for this purpose. Any deviations or contravention identified as a result of such audit/assessment would need to be rectified by the Bidder failing which the Contracting party may, without prejudice to any other rights that it may issue a notice of default.

Any publicity by the Bidder in which the name of UDI is to be used, should be done only with the explicit written permission of contracting party.

18.8 Solicitation of Employees

Both the parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party.

The above restriction would not apply to either party for hiring such key personnel who

(i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party

(ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or

(iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

18.9 Information Ownership

All information processed, stored, or transmitted by Bidder equipment belongs to contracting party. By having the responsibility to maintain the equipment, the Bidder does not acquire

implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

18.10 Sensitive Information

Any information considered sensitive must be protected by the Bidder from unauthorized disclosure, modification or access.

Types of sensitive information that will be found on UDI systems, the Bidder may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

18.11 Technological Advancements

The hardware and software proposed as part of this contract

a. should not reach end of support during the period of contract
b. should not have been announced End of Life /Sales as on the date of bid submission

In the event if the proposed hardware and software reached end of support during the period of contract, in such case the Bidder is required to replace the end of support hardware/ software with equivalent or higher capacity hardware/software at no additional cost to UDI.

18.12 Confidentiality

Bidder understands and agrees that all materials and information marked and identified by contracting party as 'confidential' are valuable assets of contracting party and are to be considered contracting party's proprietary information and property. Bidder will treat all confidential materials and information provided by contracting party with the highest degree of care necessary to ensure that unauthorized disclosure does not occur. Bidder will not use or disclose any materials or information provided by contracting party without contracting party's prior written approval.

Bidder may only disclose confidential information or use of any materials or information provided by contracting party or developed by bidder with the prior written consent of the contracting party which is:

a. possessed by bidder prior to receipt from contracting party, other than through prior disclosure by contracting party, as documented by bidder's written records;
b. published or available to the general public otherwise than through a breach of Confidentiality; or
c. obtained by Bidder from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to contracting party; or
d. Developed independently by the Bidder.

In the event that Bidder is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, Bidder shall promptly notify contracting party and allow contracting party a reasonable time to oppose such process before making disclosure.

Bidder understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause contracting party irreparable harm, may leave contracting party with no adequate remedy at law and contracting party is entitled to seek to injunctive relief.

Nothing herein shall be construed as granting to either party any right or license under any copyrights, inventions, or patents now or hereafter owned or controlled by the other party.

The confidentiality obligations shall survive for a period of one year post the termination/expiration of the Agreement.

The Bidder shall sign a Non-Disclosure Agreement (NDA) with the contracting party on mutually agreed terms and conditions. The Bidder and its antecedents shall be bound by the NDA. The Bidder shall be held responsible for any breach of the NDA by its antecedents or delegates.

The Bidder shall notify the contracting party promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of the contracting party.

18.13 Guarantees

Bidder should guarantee that all the software provided to UDI are licensed and legal. All hardware and related software must be supplied with their original and complete printed documentation.

18.14 Liquidated Damages

If the Bidder fails to meet the Project Timelines as agreed in the contract, the contracting party shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 1% (One percentage) of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the total contract price. Once the maximum is reached, contracting party may consider termination of the contract.

18.15 Termination

The Contractor party may, terminate this Contract in whole or in part by giving the Bidder a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

a. Where the Contracting party is of the opinion that there has been such Event of Default on the part of the Bidder which would make it proper and necessary to terminate this Contract and may include failure on the part of the Bidder to respect

any of its commitments with regard to any part of its obligations under its Bid, the RFP or under this Contract

b. Where it comes to the Contracting party's attention that the Bidder (or the Bidder's Team) is in a position of actual conflict of interest with the interests of the Contracting party, in relation to any of terms of the Bidder's Bid, the RFP or this Contract

c. Where the Bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against the Bidder, any failure by the Bidder to pay any of its dues to its creditors, the institution of any winding up proceedings against the Bidder or the happening of any such events that are adverse to the commercial viability of the Bidder. In the event of the happening of any events of the above nature, the Contracting party shall reserve the right to take any steps as are necessary, to ensure the effective transition of the Project to a successor Bidder / service provider, and to ensure business continuity.

d. Termination for Insolvency: The Contracting party may at any time terminate the Contract by giving written notice to the Bidder, without compensation to the Bidder, if the Bidder becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to the Contracting party

e. Termination for Convenience: The Contracting party, may, by prior written notice sent to the Bidder at least 3 months in advance, terminate the Contract, in whole or in part at any time for its convenience. The notice of termination shall specify that termination is for the Contracting party's convenience, the extent to which performance of work under the Contract is terminated, and the date upon which such termination becomes effective. In case of termination, contracting party shall pay for accepted Goods/Services completed up to the date of termination.

18.16 Consequences of Termination

a. In the event of termination of this Contract due to any cause whatsoever, the Contract with stand cancelled effective from the date of termination of this Contract
b. In case of exigency, if the Contracting party gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the successful Bidder
c. Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of the Bidder or due to the fact that the survival of the Bidder as an independent corporate entity is threatened / has ceased, or for any other reason, whatsoever, the Contracting party through re-determination of the consideration payable to the Bidder as agreed mutually by the Contracting party and the Bidder or through a Third Party acceptable to both the parties may pay the Bidder for that part of the Services which have been authorized by the Contracting party and satisfactorily performed by the Bidder up to the date of termination. Without prejudice any other

rights, the Contracting party may retain such amounts from the payment due and payable by the Contracting party to the Bidder as may be required to offset any losses caused to the Contracting party as a result of any act/omissions of the Bidder. In case of any loss or damage due to default on the part of the Bidder in performing any of its obligations with regard to executing the Scope of Work under this Contract, the Bidder shall compensate the Contracting party for any such loss, damages or other costs, incurred by the Contracting party. Additionally, the subcontractor / other members of its team shall perform all its obligations and responsibilities under this Contract in an identical manner as were being performed before the collapse of the Bidder as described above in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/any functions as stipulated by the Contracting party and as may be proper and necessary to execute the Scope of Work under the Contract in terms of the Bidder's Bid, the RFP and this Contract.

d. Nothing herein shall restrict the right of the Contracting party to invoke the Bank Guarantee and other Guarantees furnished hereunder, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to the Contracting party under law
e. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operations of the provisions of this Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

18.17 Force Majeure

Force Majeure shall mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: act of God (such as, but not limited to, fires, explosions, earthquakes, drought, tidal waves and floods);war, hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilisation, requisition, or embargo, rebellion, revolution, insurrection, or military or usurped power, or civil war, contamination by radio-activity from any nuclear fuel, or from any nuclear waste from the combustion of nuclear fuel, radio-active toxic explosive, or other hazardous properties of any explosive nuclear assembly or nuclear component of such assembly, riot, commotion, strikes, go slows, lock outs or disorder, unless solely restricted to employees of the Supplier or of his Subcontractors; or acts or threats of terrorism. Force Majeure shall not include any events caused due to acts/omissions of such Party or result from a breach/contravention of any of the terms of the Contract, Bid and/or the RFP. It shall also not include any default on the part of a Party due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Contract. However, the Bidder shall note that cyber-attack, corruption of information, software corruption, destruction of information, virus attack in the system or any such software malfunction shall not constitute a Force Majeure event and the rectification of the same shall be borne by the Bidder. The failure or occurrence of a delay in performance of any of the obligations of either party shall constitute a Force Majeure event only where such failure or

delay could not have reasonably been foreseen, or where despite the presence of adequate and stipulated safeguards the failure to perform obligations has occurred. In such an event, the affected party shall inform the other party in writing within five days of the occurrence of such event. The contracting party shall make the payments due for Services rendered till the occurrence of Force Majeure. However, any failure or lapse on the part of the Bidder in performing any obligation as is necessary and proper, to negate the damage due to projected Force Majeure events or to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate DR or any failure in setting up a contingency mechanism would not constitute Force Majeure, as set out above. In case of a Force Majeure, all Parties shall endeavour to agree on an alternate mode of performance in order to ensure the continuity of Service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure

In case of Force Majeure, all the Parties shall bear their own costs, and the contracting party shall not be liable to the Bidder for any costs that the latter incurs on account of such Force Majeure

In the event that the Force Majeure continues for 180 (one hundred and eighty) days, the Contract shall be deemed to have been terminated. If a Force Majeure situation arises, the Bidder shall promptly notify UDI in writing of such conditions and the cause(s) thereof. Unless otherwise directed by UDI, the Bidder shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

18.18 Resolution of disputes

Contracting party and the Bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project managers of contracting party and the Bidder, any disagreement or dispute arising between them under or in connection with the contract. If contracting party project manager and the Bidder project manager are unable to resolve the dispute they shall immediately escalate the dispute to the senior authorized personnel designated by the Bidder and contracting party respectively. If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the Bidder and contracting party, contracting party and the Bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration. All questions, claims, disputes or differences arising under and out of, or in connection with the contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the contract shall be referred to arbitration by a sole Arbitrator acceptable to both parties failing which the number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator who shall act as the presiding arbitrator. The Arbitration and Reconciliation Act, 1996 or any statutory modification thereof shall apply to the arbitration proceedings and the venue of the arbitration shall be New Delhi. The arbitration proceedings shall be conducted in English

language. Subject to the above, the courts of law at New Delhi alone shall have the jurisdiction in respect of all matters connected with the Contract. The arbitration award shall be final, conclusive and binding upon the Parties and judgment may be entered thereon, upon the application of either Party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides.

Continuance of the Contract: Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions under this Contract

18.19 Governing Language

The contract shall be written in the language of the bid i.e. English. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in that same language. English Language version of the contract shall govern its implementation.

18.20 Applicable Law

The contract shall be interpreted in accordance with the Indian Laws for the time being in force and will be subject to the exclusive jurisdiction of Courts at Delhi (with the exclusion of all other Courts)

18.21 Prices

The prices quoted (as mentioned in Bill of Materials submitted by the Bidder) for the solution and services shall be firm throughout the period of contract and shall not be subject to any escalation.

18.22 Taxes & Duties

Income tax shall be deducted at source by Contracting party from all the payments made to Bidder according to the Income Tax Act, unless valid and complete documents for IT exemption are submitted by the Bidder prior to release of payment. A certificate shall be provided by Contracting party to the Bidder for any tax deducted at source.

The Bidder shall bear all personnel taxes levied or imposed on its personnel, or any other member of the Bidder's Team, etc. on account of payment received under this Contract. The Bidder shall bear all corporate taxes, levied or imposed on the Bidder on account of payments received by it from the Contracting party for the work done under this Contract.

The Bidder shall bear all taxes and duties etc. levied or imposed on the Bidder under the Contract including but not limited to GST, Sales Tax, Customs duty, Excise duty, Octroi, Service Tax, VAT, Works Contracts Tax and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof during the entire Contract period, i.e., on account of material supplied and services rendered and payments received by him from the Contracting party under the Contract. However, Bidder shall recover all the Indirect taxes from contracting party

on actuals at the rate prevailing at the time of billing and contracting party shall also be responsible for any newly Introduced taxes. It shall be the responsibility of the Bidder to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. The Bidder shall also provide the Contracting party such information, as it may be required in regard to the Bidder's details of payment made by the Contracting party under the Contract for proper assessment of taxes and duties. The amount of tax withheld by the Contracting party shall at all times be in accordance with Indian Tax Law and the Contracting party shall promptly furnish to the Bidder original certificates for tax deduction at source and paid to the Tax Authorities.

If there is any reduction in taxes/duties/levies due to any reason whatsoever, after Notification of Award, the difference shall be passed on to the Contracting party. In case of increase in taxation, contracting party shall pay the tax as applicable.

The Bidder agrees that he and his Team shall comply with the Indian Income Tax act in force from time to time and pay Indian Income Tax, as may be imposed/levied on them by the Indian Income Tax Authorities, for the payments received by them for the works under the Contract

The Bidders shall fully familiarize themselves about the applicable domestic taxes (such as value added or sales tax, service tax, income taxes, duties, fees, levies, etc.) on amounts payable by the Contracting party under the Contract. All such taxes must be included by Bidders in the Commercial Bid (Bidder to find out applicable taxes for the components being proposed).

Should the Bidder fail to submit returns / pay taxes in times as stipulated under applicable Indian/State Tax Laws and consequently any interest or penalty is imposed by the concerned authority, the Bidder shall pay the same. The Bidder shall indemnify Contracting party against any and all liabilities or claims arising out of this Contract for such taxes including interest and penalty by any such Tax Authority may assess or levy against the Contracting party/Bidder.

The Contracting party shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by the Bidder at the rates in force, from the amount due to the Bidder and pay to the concerned tax authority directly

18.23 Deduction

Payments shall be subject to deductions (such as TDS) of any amount, for which the Bidder is liable under the agreement against this tender.

18.24 No Claim Certificate

The Bidder shall not be entitled to make any claim whatsoever against contracting party under or by virtue of or arising out of this contract, nor shall contracting party entertain or consider any such claim, if made by the Bidder after he shall have signed a "No Claim" certificate in favor of contracting party in such forms as shall be required by contracting party after all payments due to the Supplier are made in full.

18.25 Cancellation of the contract & compensation

Contracting party reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by it in the following circumstances:

i. The selected bidder commits a breach of any of the terms and conditions of the bid.

ii. The selected bidder goes into liquidation voluntarily or otherwise.

iii. The progress made by the selected bidder is found to be unsatisfactory

iv. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

Contracting party reserves the right to cancel the AMC placed on the selected bidder and recover AMC payment made if the service provided by them is not satisfactory.

In case the selected bidder fails to deliver the quantity as stipulated in the delivery schedule, contracting party reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility (capped at 5% differential value) of the selected bidder. After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, contracting party reserves the right to get the balance contract executed by another party of its choice by giving thirty day's written notice for the same. In this contracting party, the selected bidder is bound to make good the additional expenditure (capped at 5% differential value), which UDI may have to incur in executing the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

If the Contract is cancelled during Warranty, the bidder shall repay all the payment received from contracting party and remove the solution supplied and installed by the bidder without any extra cost to the Company. If the Contract is cancelled during AMC, contracting party shall deduct payment on pro-rata basis for the unexpired period of the contract.

18.26 Violation of terms

Contracting party clarifies that contracting party shall be entitled to an injunction, restraining order, right for recovery, suit for specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this tender document. These injunctive remedies are cumulative and are in addition to any other rights and remedies contracting party may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

19 Evaluation Methodology

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of contracting party. The pact essentially envisages an agreement between the prospective bidders/vendors

and contracting party committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract.

1. Only those bidders who qualify all Eligibility Criteria requirements shall be qualified for technical bid evaluation
2. Technical presentation shall be a part of the process for evaluation of the bids
3. The contracting party reserves the right to reject a Product/Solution/Service if it is of an opinion that the offered product/service does not match the technical requirements/objectives specified in the RFP
4. The contracting party reserves the right to request bidder for Proof of Concept (PoC) or Technical Demo for the proposed technology/solution
5. The technical bid shall first be reviewed for determining the Compliance of the Technical bids with the RFP terms and conditions, Minimum/Mandatory Technical requirements and the Scope of Work as defined in this RFP
6. Any bid found to be non-compliant to the mandatory Technical Requirements, RFP terms and conditions and the Scope of Work shall be rejected and shall not be considered for further evaluation. Bids that are technically compliant would only be taken up for commercial evaluation.
7. Bidders shall submit the detailed Technical Specifications of both hardware and software quoted by them as a part of their technical bid. Contracting party reserves right to ask for any additional specification for any hardware or software quoted by the Bidder.
8. Bidder is required to submit all the supporting documents as per the criteria mentioned in the RFP. Contracting party reserves right to summarily reject any bid which does not contain all the mandatory supporting document or may ask bidder to resubmit documents, the decision of contracting party shall be final and binding in this regard.
9. A score would be given to each bidder by contracting party based on the scoring criteria mentioned below
10. Bids that are technically qualified would only be taken up for commercial evaluation
11. Contracting party reserves the right to disqualify any bidder based on any criteria considered relevant and its decision is binding. Representations, if any from disqualified bidders shall not be entertained and shall be summarily rejected. Contracting party shall not respond to any query raised by bidders seeking reasons for rejection of the bid.
12. A technical bid to commercial bid evaluation criteria of 80% to 20% will be applied.

19.1 Technical Evaluation

The evaluation of technical proposals, among other things, will be based on the following:

S.No.	Technical Evaluation	Evaluation Criterion Details	Max. Marks Allotted	Supporting Documents Required
A. Bidder's profile (max. -150 marks)				
A1	Average annual turnover	Average annual turnover over the last three financial years (FY 2019-20, 2020-21 and 2021-22). Marks shall be allotted as given below: - More than INR 250 Crores = 90 marks - More than INR 100 Crores – up to INR 250 Crores = 60 marks - More than INR 50 Crores – up to 100 Crores = 30 marks	90	Certificate from the Statutory Auditor on turnover details from the over the last three (3) financial years
A2	Manpower	Full time employees on payroll of the Bidder, working in the business unit providing "IT/ITeS" as on bid submission date. Marks shall be allotted as given below: - More than 300 full-time employees = 60 marks - Between 150 – 300 = 30 marks - Between 100 – 150 = 20 Marks	60	Certificate from the Head of HR Department or equivalent on bidding entity's letter head countersigned by authorised signatory for this bid holding written special power of attorney on stamp paper
B. Project Experience (max. -500 marks / 10 Projects) **Please Note: 50 marks shall be assigned against each project (maximum 3 projects to be shown against each category B1 to B4 as defined below) and same project shall not be considered in different categories.**				
B1	Software Maintenance, modifications & enhancements of any National/ State e-Governance or a similar type of application	The Bidder should have experience in India of executing software maintenance, modifications & Enhancements of any National/ State e-Governance or a similar type of application and providing its repository infrastructure each having a minimum value of INR 10 Crores, out of which one (1) project should have been completed during the last 5 years as on bid submission date		- Work order OR - Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract/ order AND - Completion Certificate issued & signed by the

S.No.	Technical Evaluation	Evaluation Criterion Details	Max. Marks Allotted	Supporting Documents Required
				competent authority of the client entity on the entity's letterhead ***Note:*** *In case of a turnkey project comprising of application development and IT Infrastructure, the Bidder is required to submit a certificate from Statutory Auditor specifying value of the respective business area*
B2	Software Maintenance, modifications & enhancements of any **Core Banking/ Insurance System application** (including IT Infrastructure and licenses) with minimum 50 Lacs transactions per year in any year of project duration	The Bidder should have experience in India of executing software maintenance, modifications & enhancements of any **Core Banking/ Insurance System application** (including IT Infrastructure and licenses)" each project having minimum value of INR 10 Crores out of which one (1) project should have been completed during the last 5 years as on bid submission date		Work order **OR** -Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract/ order **AND** -Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead ***Note:*** *SLA report certified by the Client mentioning number of transactions for Financial / Core Banking System application projects*
B3	Software Maintenance, modifications & enhancements of any **IT Registry System** which	The Bidder should have experience in India/Abroad of executing software maintenance, modifications & enhancements of any **IT Registry System** which can be integrated with external systems with at least 05 million		-Work order **OR** -Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order **AND** -Completion Certificate

S.No.	Technical Evaluation	Evaluation Criterion Details	Max. Marks Allotted	Supporting Documents Required
	can be integrated with external systems	records each project having minimum value of INR 10 Crores out of which one (1) project should have been completed during the last 5 years as on bid submission date		issued & signed by the competent authority of the client entity on the entity's letterhead ***Note:*** *Self-certificate for number of records in the IT Registry System from the bidder signed by the concerned project manager of the bidder and counter signed by authorised signatory for this bid holding written special power of attorney on stamp paper along with the official contact details of the competent authority of the client entity*
B4	Supply, Installation, Operations and Maintenance of networking equipment, storage backup equipment, servers and cyber-security	The Bidder should have experience in India of executing supply, installation, operations and maintenance of networking equipment, storage backup equipment, servers and cyber-security each having minimum value of INR 10 Crores out of which one (1) project should have been completed during the last 5 years having as on bid submission date		-Work order **OR** -Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order **AND** -Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead
C. Approach, methodology & efficiency of the proposed solution framework (max. -250 marks) - To be evaluated after submission and presentation				
C1	Approach, Methodology & Solution	Overall approach, modularity and efficiency of the solution	**30**	
		Infrastructure design including horizontal scalability	**25**	

S.No.	Technical Evaluation	Evaluation Criterion Details	Max. Marks Allotted	Supporting Documents Required
		Ease of Integration and Analytics	**25**	
		Definition of sample APIs, data models and Management of APIs	**20**	
		High availability	**20**	
		Security of the solution	**20**	
		Data quality management and SLA monitoring	**20**	
		Agile development strategy	**20**	
		Operations and Management plan	**20**	
C2	Presentation	Qualified bidders shall be called for presentation and presentation shall be delivered by the proposed Project Manager assisted by Team Lead/s (Assessment to be based on a note covering all requirements as mentioned above & Presentation made by the Bidder before the Contracting Party)	**50**	
D. Proposed resources (max. -100 marks)				
D1	Resources (for evaluation purpose)	**Design, Development & Implementation Phase:** 1. Project Manager – 12.5 marks 2. Functional Expert – Registry – 7.5 marks 3. Team Leader (Application Software Expert) – 7.5 marks 4. Team Leader (IT Expert) – 7.5 marks 5. IT Security Expert – 7.5 marks 6. Network Administrator – 7.5 marks 7. System Administrator – 7.5 marks		Manpower Details in Bid Submission document

S.No.	Technical Evaluation	Evaluation Criterion Details	Max. Marks Allotted	Supporting Documents Required
		8. Database Administrator – 7.5 marks 9. Application Development Expert – 5 marks 10.Quality Assurance Lead – 5 marks **Operations & Maintenance Phase:** 1. Project Manager – 5 marks 2. Team Lead (IT Expert) – 5 marks 3. Team Lead (Application Software Expert)- 5 marks 4. IT Security Expert – 5 marks 5. Database Administrator – 5 marks ***Note:*** *All the proposed resources shall be full time employee of the Bidder.*		

The Technical Evaluation would be done for only those bidders, who comply with the eligibility criteria mentioned in Section 18.27 – Evaluation of Eligibility Criteria. The Evaluation Committee may invite only such qualified bidders to make a presentation as part of the technical evaluation.

Only those bids which have a minimum technical score of 80% of total marks shall be considered qualified. However, contracting party reserves the right to lower the minimum required marks if none of the bidders achieves 80% of the total technical marks. The bid complied as per criteria mentioned above shall be evaluated as per the framework detailed below:

S. No.	Evaluation Criteria	Marks
1	Bidder's profile	150
2	Project Experience	500
3	Approach, methodology & efficiency of the proposed solution framework	250

4	Proposed resources	100
5	**Total Marks**	1000
6	**Minimum Qualifying Marks**	800

Evaluation of Resources (Annexure II: Manpower Details in Bid-submission document)

A	**GENERAL QUALIFICATIONS**	**20%**
A1	Technical qualifications	10%
A2	Professional experience	5%
A3	Industry Certifications	5%
B	**ADEQUACY FOR THE ASSIGNMENT**	**65%**
B1	Experience in similar capacity / broad sector	25%
B2	Experience relevant to RFP/Project	40%
C	**ASSOCIATION WITH THE COMPANY**	**15%**
C1	Full Time permanent staff	12%
C2	Years of association	3%

1. If any experts get less than 60% marks then he need to be replaced at the time of negotiation
2. The CVs for only evaluation purpose shall be required to be submitted with the proposal
3. If any of the experts are unavailable for the extended validity period, the Bidder shall provide a written adequate justification and evidence satisfactory to contracting party together with the substitution request. In such a case, replacement expert shall have equal or better qualifications and experience than those of the originally proposed expert. The technical evaluation score, however, shall remain to be based on the evaluation of the CV of the original expert.
4. If the Bidder fails to provide a replacement expert with equal or better qualifications, or if the provided reasons for the replacement or justification are unacceptable to contracting party, such proposal shall be rejected by contracting party
5. Except as contracting party may otherwise agree in writing and no changes shall be made in the experts without the prior consent of contracting party
6. A request for substitution of expert during the term of the Contract may be considered based on the Bidder's written request
7. contracting party may make a request in writing for the substitution of an expert with an equal or better qualification and experience. On receiving request, the Bidder shall provide substitution within 30 days of receipt of request for the respective expert.

8. In case any proposed resource resigns, then the Bidder has to inform contracting party within one week of such resignation and the bidder shall promptly initiate a search for a replacement to ensure that the role of any member of the expert is not vacant at any point in time during the contract period, subject to reasonable extensions requested by the bidder and its approval by contracting party
9. If contracting party finds that any of the personnel has committed serious misconduct or has been charged with having committed a criminal action, or if contracting party determines that bidder's personnel have engaged in any corrupt, fraudulent, coercive, collusive, undesirable or restrictive practices while performing the work, the bidder shall at contracting party's written request, provide a replacement for such personnel
10. The replacement of any personnel shall possess equivalent or better qualifications and experience and shall be approved by contracting party

The commercial proposals of technically short-listed Bidders will then be opened.

19.2 Commercial Evaluation

The commercial bids for the technically qualified Bidders will be opened and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at UDI's discretion. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of three years.

Technical committee in consultation with contracting party will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the mix of L1 & technical scoring (80%), provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

20 Service Level Agreement

Bidder shall ensure compliance with the SLAs defined in the RFP. This section describes the service levels that has been established for the services offered by the bidder to contracting party. The bidder shall monitor and maintain the stated service levels to provide quality customer service to contracting party.

20.1 System Availability

System availability is defined as {(Scheduled operation time - system downtime)/ (scheduled operation time)} *100%, where:

- Performance for availability service level default would be measured on monthly basis.

- "Scheduled operation time" means the scheduled operating hours of the system for the year. All planned downtime would be deducted from the total operation time for the year to give the scheduled operation time.
- "System downtime" subject to the SLA mentioned in this RFP, means accumulated time during which the system is totally in-operable due to in-scope system or infrastructure failure, and measured from the time contracting party and / or its customers log a call with bidder's help desk of the failure or the failure is known to bidder from the availability measurement tools to the time when the system is returned to proper operation.
- UDI has critical and key infrastructure of DC and DR to be monitored on a 24*7 basis.
- Uptime will be for each individual server.
- Response may be telephonic or onsite depending on the criticality and how the SLA stands as per this RFP.

If any one or more of the proposed components at DC, NDR or DR are down resulting in non-availability of UDI server hardware, then downtime will be calculated as mentioned in the below section.

20.2 Issue Criticality Classification

The classification strategy has been envisaged to prioritize problem resolution based on contracting party priorities rather than in an ad-hoc manner. Classification framework will help contracting party and the bidder to develop a shared understanding of the issue at hand, as well as the anticipated response and resolution timelines.

In order to improve the accuracy of the classification of an issue, application specific performance thresholds have been defined based on two characteristics, as mentioned below:

Impact: Number of users getting affected by the issue

Availability: Uptime of the system, both, in absolute terms as well as percentage terms

- In case of a disaster at DC or DR drill, DR would be the primary site and then, infrastructure at DR shall be considered as Critical and penalty shall be computed accordingly
- If any hardware (server etc.) in High Availability (HA) mode or tape library fails while other is working with no impact on the availability of the underlying solution/application, in such a case, penalty shall be levied on the failed hardware. The failed hardware in HA mode should be replaced within 12 hours of the failure. If the bidder fails to meet the timeline, contracting party shall levy a penalty
- If both the hardware components fail in HA mode, contracting party shall levy penalty on the bidder for the service levels defaults, basis the service levels requirement mentioned here.

- For three (3) downtime occurrences within a stipulated time window of a calendar month, a sum equivalent to 1% of the product cost of the respective product would be levied as a penalty. This would be over and above the monthly service level default penalty.

20.3 Service Level Default

As mentioned above, Service Level measurement would be on monthly basis. Bidder's performance will be assessed against Minimum Expected Service Level requirements mentioned in the Availability measurement table.

An availability service level default will occur when, the bidder fails to meet Minimum Service Levels, as measured monthly, for a particular Service Level.

Availability: -

Will be calculated as below

Availability = (U - C - D)/ (U - C)

System Scheduled Uptime for servers (U)

Scheduled Downtime for servers (C)

Unscheduled Downtime for servers (D)

Service Level Description	Minimum Service Level	Measurement Tools	Cost Reference for the Contract Period
Availability of Critical Infrastructure and software	99.99%	Enterprise Management System	Product cost at DC + Installation cost at DC + AMC & ATS cost at DC
Availability of Key Infrastructure and software	99.3%	Enterprise Management System	Product cost at DR + Installation cost at DR + AMC & ATS cost at DR
Availability of Significant Infrastructure and software	99%	Enterprise Management System	Product cost of standalone server + Installation cost at standalone server + AMC & ATS cost of standalone server
Availability of Individual components not impacting availability of the server/solution infrastructure	96.7%	Helpdesk/Enterprise Management System	For every hour of delay thereof, penalty shall be levied at the rate of INR 5000

Infrastructure and application Support

Response comprises acknowledgement of the problem and an initial analysis of the underlying cause

Uptime - The amount of time that the system is available for normal use. (Do note that planned maintenance would also be classified as normal use.)

All the cost of the hosting all the environment as mentioned in the RFP needs to factor by the bidder in the Commercial bill of material with proper details and break up.

Critical Level	Response Time	Resolution Time
Critical Infrastructure and software	5 Min	Within 2 Hrs of call reporting
Key Infrastructure and software	5 Min	Within 4 Hrs of call reporting
Significant Infrastructure and software	5 Min	Within 6 Hrs of call reporting
Individual components not impacting availability of the server/solution infrastructure	5 Min	Within 8 Hrs of call reporting

Service Level Description	Measurement	Minimum Service Level	Measurement Tool	Penalty
Hardware Utilization	Reporting to the UDI if Hardware daily peak utilization levels of CPU, RAM, NIC and hard disk etc. exceeds 70% (Seventy Percent) at any given point of time during business hours. Each incident should not exceed 5 minutes, every part thereof will be a new incident.	100%	Manual / Tool	If less than 3 times: for every 0.5% drop in service level, Penalty of 1% of the respective Hardware Cost If more than 3 times in a quarter: Bidder will be responsible for replacing/augmenting the hardware at no additional cost to the UDI within 3 months of exceeding the thresholds.

				Incase bidder fails to replace the hardware, LD of 1% of effected product cost will be lived for every week of delay or part thereof
Storage Utilization	Production storage utilization levels exceeds 80% (Eighty percent) at any given point of time and such incidents occurs for more than 3 times in a quarter. Each incident should not exceed 5 minutes, every part thereof will be a new incident	100%	Manual / Tool	If less than 3 times: for every 0.5% drop in service level, Penalty of 1% of the respective Hardware Cost If more than 3 times in a quarter: Bidder will be responsible for replacing/augmenting the hardware at no additional cost to the Bank within 3 months of exceeding the thresholds. Incase bidder fails to replace the hardware, LD of 1%of effected product cost will be lived for every week of delay or part thereof
Software Service Request	Percentage of Software Service Requests concluded (software installation, patches, bug fixes, errors) within defined timeframe/response-resolution window.	100% per instance	Manual / Tool	INR 5000 for every instance of delay
Incident Management	Percentage of incidents escalated	100% per instance	Manual / Tool	INR 5000 for every instance of delay

	according to the Incident Management matrix (as shown in Incident Matrix Table below)			
Downtime for servicing	• Each planned down - time for system servicing (up gradation, bug fixing, patch uploads, regular maintenance etc.) will not be more than 4 hours. • This activity will not be carried out during business hours. • However, such activities which require more than 1 hour or required to be carried out during business hours, will be scheduled in consultation with contracting party. In case, downtime exceeds the planned hours, the additional time taken for servicing will be considered for infrastructure or system downtime as per availability measurements table.	100% per instance	Manual / Tool	INR 5000 for every 1 hour of delay above the scheduled downtime
Modification (Customization / Enhancements) resolution for Application	Bidder to ensure that all modifications, enhancements reported by the contracting party and mutually agreed with	96%	Manual / Tool	Monthly AMC / ATS of the affected services

software	the bidder will be duly sized and resolved as per the defined timeframes			
UAT Bug Resolution	Bidder is required to ensure that all bugs reported by testing team during UAT will be duly resolved within defined timeframe	96%	Manual / Tool	Monthly AMC / ATS of the affected services
Backup Success Rate	Bidder needs to maintain 100% backup success rate	100%	Manual / Tool	• INR 500 for every daily backup/backup restoration failure • INR 1000 for every weekly/monthly backup/backup restoration failure • INR 5000 for every quarterly backup/backup restoration failure • INR 10000 for every yearly backup/backup restoration failure
Backup Window	If bidder quotes new backup software solution, then bidder has to maintain a backup window of 5 hours	100%	Manual / Tool	<= 1 instance - No Charges >1 Instance - INR 1000 for every additional instance of Backup default
Patch Management	Patch management solution should be functional at any given point of time, on 90% of the device/server /application/endpoints	Per Instance	Manual / Tool	Penalty of INR 25,000 for every instance of default provided the default is due to bidder/product

DR Drill	NO of successful DR Drill conducted by the bidder	100%	ADR Tool	Penalty of INR 1,00,000 for every instance of default provided the default is due to bidder/product
RTO and RPO maintenance	Maintenance of RTO and RPO as mentioned in the RFP	100%	ADR Tool	Penalty of INR 1,00,000 for every instance of default provided the default is due to bidder/product
Content Uploading and Content Removal	Within 4 hours from the requested time.	100%	Manual	Above 4 hours within 8 hours: 10,000 Above 8 hours: 50,000

Database & Application Response Assessment

Service Level Description	Measurement	Minimum Service Level	Measurement Tool	Penalty
Database Response Assessment	End to End response time within DC (from the Core Insurance Application and UDI web-based platform to the respective Database and back) should be <10 ms (mile seconds) during business hours	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the overall cost of the hardware in TCO.
Application response time	This is the time taken from submission of any request by end-user – to - response of the request to the end user Response time < 2 sec	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the overall cost of the hardware in TCO

Page Transition	Time taken for page transition Response time < 2 sec	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the overall cost of the hardware in TCO

Management, Reporting and Governance

Service Level Description	Measurement	Minimum Service Level	Measurement Tool
Program Manager and Service delivery Manager	No change in these resources for minimum 1 year from the contract date and maximum 2 changes in the complete contract term (*the Program Manager should not be rotated to other clients of the Service Provider under the contract period).	100%	Manual
Staff transition period (Handover period)	60 days for any personnel associated with the project	100%	Manual
Resource availability	Attendance for support personnel, L1 and L2 engineers. (covers all the locations) Minimum attendance level on any day is 90% of agreed deployment.	No of days below minimum attendance level	Manual

Overall cap of all the penalties over the tenure of the contract will be 10% (ten percent) of the contract value.

Service Levels will be applicable for the respective Hardware and Software once the Same is accepted and Go-live

20.4 Penalty Computation

In the event of Service Level Default, bidder shall pay contracting party a penalty that will be computed in accordance with the following formula:

Monthly Service Level Default = Minimum Service Level (for a month) – Actual Service Level (for a month)

Total amount of penalty, bidder is obligated to pay contracting party, shall be reflected on the invoice provided to contracting party in the quarter, after the quarter in which the Service Levels were assessed. Contracting party shall be entitled to deduct the penalty amount from the amounts payable by them to the selected bidder as per the invoice.

20.5 Project Timelines

The scope of work is divided in different areas and the payment would be linked to delivery and acceptance. All / any payments will be made subject to compliance of Service Levels defined in the RFP document. The contracting party shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of contracting party. If any of the items / activities as mentioned in the price bid is not taken up by contracting party during the course of the assignment, contracting party will not pay the fees quoted by the Bidder in the price bid against such activity / item.

Payment for the Supply of required Cloud, Software, Design, Installation, Implementation, and Commission of the solutions shall be made by UDI as per the solutions in scope as mentioned in the Scope of Work.

RFP – Time Schedule

S. No.	Particulars	Date & Time	Day
1.	RFP Document made available for Bidders	***05.05.2022***	***Thursday***
2.	Last date & time for receiving written queries from Bidders	***20.05.2022***	***Friday***
3.	Date & time of Pre-Bid meeting of Bidders with Contracting Party, Mumbai on RFP Document	***21.05.2022*** ***3:00 pm***	***Saturday***
4.	Date for issuing clarifications by the Contracting party to the to the queries raised by the Bidders	***22.05.2022***	***Sunday***
5.	Last date and time for submission of Technical Proposal and Financial Proposal	***6.06.2022*** ***12:00 Noon***	***Monday***
6.	Date & time for opening of the Technical Proposal	***7.06.2002*** ***12:00 Noon***	***Tuesday***
7.	Date & time for Presentations (To be communicated individually to the Eligible Bidders)	***08.06.2022 to 09.06.2022***	***Wednesday to Thursday***

8.	Date & time for opening of the Financial Proposal and declaration of Selected Bidder	***13.06.2022 12:00 Noon***	***Monday***
7.	Place of Submission and Opening the Proposal	***Project Office - General Insurance Council 5th Floor, National Insurance Bldg, 14, J Tata Road, Churchgate, Mumbai - 400020***	

List of Activity Tracks, Deliverables and Timelines

Sl. No	Milestone	% of Fees Payable	Timelines
1.	Signing of Contract with contracting party		T
2. PART A Deliverable Signoff by contracting party including completing of the following: **Part A Go-Live is expected by 25th May 2022**		30% (On completion of point no. 2 to 3)	
2.1	Approval of contracting party web-based platform Requirements Specification & Migration Plan Document • Detailed System Study, finalization of detailed list of activities, scope and duration of each of the activity and • submission of detailed project plan • Deployment Plan Document • Change Management Methodology Document		T + 20 days
2.2	Delivery of Hardware, License for Test & Development environment & Installation		T + 20 days
2.3	Training to department Officials on Content Management		T + 20 days
2.4	On successful completion of UAT as per existing features and functionalities • Detailed Use Cases and Activity diagrams • High Level Architecture Document • Techno – Functional Risks and Mitigation Document • Functionality Traceability matrix • High Level Design Document • Low Level Design Document • Test Plans		T + 20 days
2.5	Delivery of License for production environment & Installation		T + 20 days
2.6	Design Document and Source Code		T + 20 days

2.7	Safe to Host Certificate / Security and Regulatory compliances		T + 20 days
2.8	Launch of New UDI web-based platform on Production Environment as per existing features and functionalities • Development, Testing and Presentation of the Final version • Release Notes		T + 35 days
2.9	Data input of current active policies (Details in section 9.3)		T + 35 days
3. PART B Deliverable Signoff by contracting party including completing of the following:			
3.1	Data Migration (Details in section 10.1)		T + 45 days
3.2	Deduplication (Details in section 10.2)		T + 45 days
3.3	Search Engine (Details in section 10.3)		T + 45 days
4. PART C Deliverable Signoff by contracting party including completing of the following:		30% (On completion of point no. 4 to 5)	
4.1	Configuration Management (Details in section 11.1)		T + 60 days
4.2	MIS/ Reporting and creation of Live dashboards (Details in section 11.2)		T + 60 days
4.3	Archiving (Details in section 11.3)		T + 60 days
4.4	Grievance Management (Details in section 11.4)		T + 60 days
5. Part D Deliverable Signoff by contracting party including completing of the following: (Details in section 12) APIs between UDI & stakeholder entities: API integration between Bank & UDI API integration between UDI & Centralized Repository API integration between UDI & Insurer API integration between UDI & and any other application			
5.1	API integration between Top 5 participating Insurers and their partner Banks		T + 45 days
5.2	API Integration with the Rest of parties/ External applications		T + 45 days
5.3	Aadhar vault		T + 60 days
6	Two (2) Months of successful running of UDI web-based platform on Production Environment post go Live of PART D deliverables signoff from UDI	10%	
7	On completion of 12 months period of warranty post PART D deliverable signoff from contracting party	10%	
8	On completion of 24 months period of warranty post PART D deliverable signoff from contracting party	10%	
9	On completion of 36 months period of warranty post PART D deliverable signoff from contracting party	10%	

Mode of Payment

Contracting party shall make all payments only through Electronic Payment mechanism (*viz.* ECS).

Glossary	
1. RFP	Request for proposal
2. IT	Information Technology
3. PMJJBY	Pradhan Mantri Jeevan Jyoti Bima Yojana
4. PMSBY	Pradhan Mantri Suraksha Bima Yojana
5. UDI	Unified Digital Interface
6. DFS	Department of Financial Services
7. GOI	Government of India
8. GI COUNCIL	General Insurance (GI) Council
9. LI COUNCIL	Life Insurance (LI) Council
10. IBA	Indian Banks' Association
11. RRB	Regional Rural Banks
12. IRDAI	Insurance Regulatory and Development Authority of India
13. RBI	Reserve Bank of India
14. NABARD	National Bank for Agriculture and Rural Development
15. SEBI	Securities and Exchange Board of India
16. DC	Data Center
17. DRC	Data Recovery Center
18. OEM	Original Equipment Manufacturer
19. PSU	Public Sector Unit
20. SLA	Service Level Agreement
21. MIS	Management Information Systems
22. COI	Certificate of Insurance
23. CA	Chartered Accountant
24. BPM	Business Process Management
25. WFMC	Workflow Management Coalition
26. W3C	World Wide Web Consortium
27. SOAP	Simple Object Access Protocol
28. REST	Representational State Transfer
29. HTTP	HyperText Transfer Protocol
30. PKCS	Public Key Cryptography Standards
31. ISO	International Organization for Standardization
32. ITIL	Information Technology Infrastructure Library
33. EITM	Enterprise IT Management
34. IEEE	Institute of Electrical and Electronics Engineers
35. UI/UX	User Interface/ User Experience
36. API	Application Programming Interface
37. SMS	Short Message Service
38. DB	Database
39. IIS	Internet Information Services
40. CI/CD	Continuous Integration/Continuous Delivery
41. ISNP	Insurance Self Networking Platform
42. ISMS	Information Security Management System
43. VAPT	Vulnerability Assessment and Penetration Testing
44. WASA	Web Application Security Assessment
45. SIEM	Security Information and Event Management

46. I/O	Input – Output
47. TLS	Transport Layer Security
48. AES	Advanced Encryption Standard
49. NSDL	National Securities Depository Limited
50. SMTP	Simple Mail Transfer Protocol
51. JSON	JavaScript Object Notation
52. XML	Extensible Markup Language
53. ETL	Extract, Transform, Load
54. SOP	Standard Operating Procedure
55. BCP	Business Continuity Planning
56. SRS	Software Requirements Specification
57. APM	Application Performance Management
58. DRaaS	Disaster Recovery as a Service
59. DNS	Domain Name System
60. GSLB	Global Server Load Balancing
61. UAT	User Acceptance Testing
62. SIT	System Integration Testing
63. OS	Operating System
64. SSL	Secure Sockets Layer
65. UIDAI	Unique Identification Authority of India
66. SAN	Storage Area Network
67. RAID	Redundant Array of Independent Disks
68. RDBMS	Relational Database Management System
69. LDAP	Lightweight Directory Access Protocol
70. SQL	Structured Query Language
71. DBMS	Database Management System
72. DDL	Data Definition Language
73. RISC	Reduced Instruction Set Computer
74. EPIC	Explicitly Parallel Instruction Computing
75. SOC	Security Operations Center
76. MSP	Managed Service Provider
77. CSP	Cloud Service Provider
78. HSM	Hardware Security Module
79. KMS	Key Management Service
80. AI	Artificial Intelligence
81. ML	Machine Learning
82. RTO	Recovery Time Objective
83. RPO	Recovery Point Objective
84. IPv4	Internet Protocol version 4
85. IPv6	Internet Protocol version 6
86. FAQ	Frequently Asked Questions
87. CBS	Core Banking Solution
88. CRM	Customer Relationship Management
89. KYC	Know Your Customer
90. KUA	KYC User Agency
91. EOD	End of Day
92. BOD	Beginning of Day
93. AMC	Annual Maintenance Contract
94. ATS	Annual Technical Support
95. FM	Facility Maintenance

96. STQC	Standardization Testing and Quality Certification
97. HLD	High Level Design
98. LLD	Low Level Design
99. GST	Goods and Services Tax
100. VAT	Value Added Tax
101. TDS	Tax Deducted at Source