Request for Proposal

For

Industry-wide Fraud Analytics System

Part – 1:: Requirements and Instructions

Insurance Regulatory and Development Authority

3rd Floor, Parishram Bhavan, Basheerbagh,

Hyderabad – 500004.

Contents

List of Abbreviations Used

Abbreviation	Description
IRDA	Insurance Regulatory and Development Authority
IIB	Insurance Information Bureau of India
FAS	Industry wide Fraud Analytics System
TPA	Third Party Administrators
PAN	Permanent Account Number issued by Income Tax Authorities
RPO	Recovery Point Objective
RTO	Recovery Time Objective
DC	Data Center
DR	Disaster Recovery Center
BCP	Business Continuity Process
BAP	Business Analytics Project of IRDA
CIBIL	Credit Information Bureau of India Limited
SOP	Standard Operating Procedure
SAN	Storage Area Network
SRS	System Requirements Specification
TDD	Technical Design Document

Section 1 :: Introduction to IIB:

Insurance Regulatory and Development Authority has constituted the Insurance Information Bureau of India (IIB), an advisory body which is collecting, processing and disseminating data. IIB has been formed to ensure that the business data of insurance companies is collected and processed in an orderly manner and is made available at regular intervals. The data so collected is useful for the various market players, researchers, policyholders as well as the public at large for decision making.

IIB functions as a single point official reference for the entire data requirements on the insurance sector. The decisions regarding processing and dissemination of data are undertaken as per the policy laid down by the Bureau. All Non-Life insurers are required to upload the insurance data on motor, health and other lines of business online as per the data formats prescribed by IRDA. As part of this initiative, summarized data for the Health insurance segment as a whole will be made available to the insurers for making better decisions on proposals for insurance and on claims.

Transaction level data for several lines of business (including health insurance business) is currently being collated at the IIB for various analytics purposes. The transactional data with respect to the Health insurance business also is being collated at the IIB. The health insurance transactions are transmitted to the IIB by all Non-life insurers/Life insurers/TPAs on a monthly basis via a batch mode in a text file as per the prevailing practice.

The prescribed formats used for sending the data can be seen at https://iib.gov.in/IRDA/datamanuals/Data%20formats.htm.

Sample transaction level data on Health insurance can be obtained from the link below:

https://iib.gov.in/IRDA/Sample_Transaction_levelData_Health.html.

Currently, the analytics are being developed manually and sample analytics can be found in the “Public reports” section of the IIB’s website (www.iib.gov.in). However, it may be noted that these analytics are for general business purposes and not for identifying a fraud.

Section 2 :: Business requirements:

IRDA intends to reduce the cost of fraud by building advanced detection and prevention systems at Industry level by leveraging all available information.

The initiative is expected to identify fraudulent claims at claim processing stage before payment occurs and improve the accuracy of fraud detection. The initiative is also intended to assist the Insurers with better screening of proposals at underwriting stage and also in handling claims. The system is expected to ensure that the insurers are empowered to take informed decisions on underwriting and claims with the help of the predictive and analytical capabilities. Thus, the origination and payment stages of policy life cycle are brought under the radar. The supporting inputs for underwriting of proposals and claim processing may be transmitted through web-services, notifications, emails and/or role based access to the solution provided to Insurers/TPAs.

The solution would aim at throwing up suspicious behavior patterns by way of alerts and provide information such as scores, which will help Insurers streamline and prioritize cases for Investigation and improve operational efficiencies of Fraud Investigation units.

The initiative is expected to help Insurers minimize anti-selection and will provide access to information which supplements the basis on which coverage is offered. Thus, the initiative will accelerate processing of applications and also reduce costs thereby improving the product pricing. Through the Fraud Analytics system, it is envisioned that the initiative of Multi-disciplinary solution would motivate the Insurers to look at existing underwriting and claims' processes and ascertain potential areas where fraud detection capabilities need to be put in place.

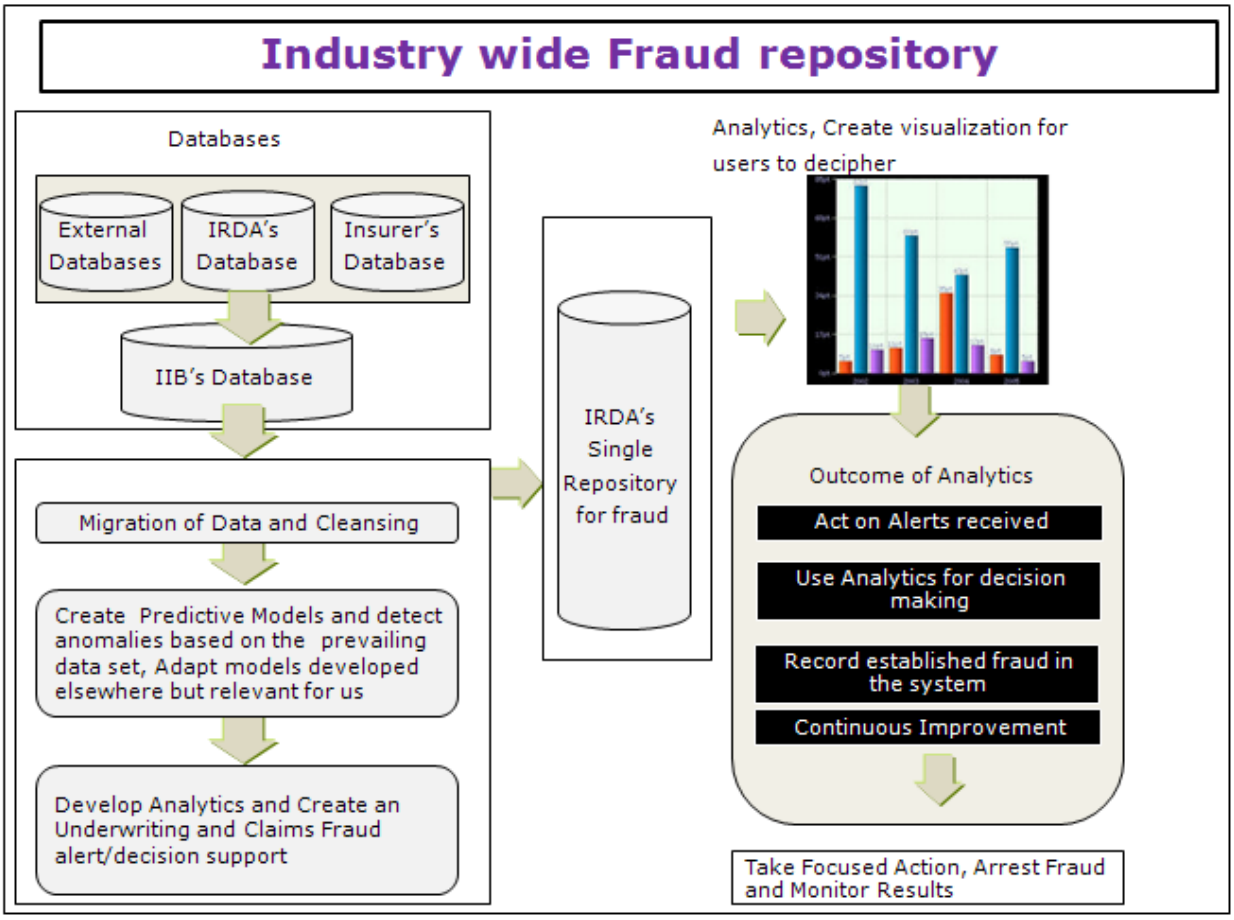
The project aims at establishing an industry wide fraud database that will eliminate the need for the individual insurers to set up software and hardware solutions at an entity level. Advanced statistical and artificial intelligence techniques used as part of this initiative would help find patterns that traditional tools may not reveal. The development of a central repository for frauds in the country will have the capability to develop and improve models and generate all possible kinds of triggers, alerts and analytics for the purposes of fraud prediction and detection. It is proposed to use the statistical techniques in classification, forecasting, optimization and simulation areas for building models to generate analytics for prevention and detection of fraud.

It may be noted that the IIB currently receives transaction level data in a periodic batch cycle. The vision of the project is to move towards real time transaction level data integration with IIB so as to build a robust and effective real time fraud prevention and analytics system. By enabling Insurers with real time capabilities for decision making information to prevent fraud, the initiative is expected to help the Industry save money and achieve higher efficiency.
IRDA is looking at the firms/ organizations to submit a proposal to establish a comprehensive solution for Insurance fraud management which would assist both the Regulator and Industry with emphasis on Indian insurance environment. The solution shall

- Enable the Insurers to underwrite the proposals effectively by obtaining the required information, fraud alerts and history from the central database and also enable experience studies on products based on reliable database.

- Assist the Insurers efficiently manage the claims so that genuine customers do not face hassles by obtaining relevant information on fraud and claim reporting patterns
- Help develop a vibrant market place in health Insurance space

The diagrammatic representation of the proposed initiative is given hereunder:



While the RFP proposes an indicative list of features/triggers/requirements for this solution, it is expected that the bidder proposes a solution that caters to the widest possible range of features as a part of the Fraud Analytics Framework.

Also, while the bidder brings the statistical and mathematical models as well as other tools such as profiling, scoring etc for anomaly detection and predictive capabilities, they need to work with IRDA/IIB to draw a data policy for the solution implementation and plan data. They may need to work with IRDA/IIB in data formats standardization across Health space, if any, and identify knowledge databases and third party databases for improving the models and analytics.

It is expected that the bidder brings to the table expertise on both Fraud management process experience and skills of Insurance Fraud solution implementations. The bidder is expected to partner with IRDA/IIB for implementing and improving the solution by continually modifying statistical& technological models/frameworks and in assisting interpretation and analysis of the results. The bidder

is also expected to build capacity of IRDA/IIB to build, operate and maintain the solution for the contract period at IIB's data center.

Section 3 :: Functional requirements

3.1. Single repository for Fraud:

3.1.1. The solution should create and maintain a single repository of Frauds. This repository needs to capture the complete characteristics and details of fraud and facilitate seamless flow of such information among Insurers/TPA's to prevent loss due to fraud.

3.1.2. The repository should support large amount of data from all stakeholders in Health Insurance system and support online access of the application and real-time, query-response ways of information exchange.

3.1.3. The design of the repository should enable the framework to support collection of the required data on occurrence of incidents, the modus operandi, perpetrators/collaborators and the alarms and every piece of information that is relevant to model effective fraud prediction/detection. In addition, for any fraud that is detected outside this system, adequate enablement shall be provided to the insurers/TPA's to manually enter/automatically export such data into this system.

3.1.4. The repository needs to accumulate historical information of deviations/anomalies etc and abstract trends and implications.

3.1.5. The repository design should support integration of other databases maintained by different Regulators, Government departments like police, crime branches etc and hospitals or any agency (ies) that cater to the health segment. This includes other databases established for the purpose of fraud detection/prevention. This integration, it is believed, will enable the exchange of data and results of analysis amongst organizations/agencies combating fraud.

3.1.6. The repository should be robust and capable of identifying new generation frauds. The support for ongoing/dynamic changes keeping in view, the emerging fraud trends' shall also be provided.

3.1.7. The repository shall provide the capability to run a look up on the complete database to identify any earlier instance of unnoticed fraud/suspicious activity using any newly acquired intelligence (system/human)/analytical abilities/experience gained. The administrators of the system shall be given capabilities (screens, tools, commands etc.,) to run these models/tools and identify past instances of un-detected fraud/suspicious activity.

3.1.8. The repository should maintain the history of all the frauds identified and established by the insurer(s) or by any other agency, irrespective of whether the fraud is alerted by the repository or otherwise.

3.2. Modeling with Anomaly detection capabilities:

The solution is envisaged to provide predictive analytics support with the help of the modeling techniques (including classification, forecasting, simulation and optimization techniques). The modeling techniques generally rely on supervised learning based on the past cases of established fraud to classify and predict a future possibility. However, due to the absence of a well-established health insurance frauds' database within the country, it could be pertinent to utilize any insight from the experiences gained in health domain in a different geography that is still relevant and meets our country's purpose. The bidder is expected to bring this experience and knowledge to the table for the purpose of building an effective modeling framework in consultation with IIB/IRDA.

Hybrid modeling that is partly based on

- the insights gained in different geographies
- unsupervised learning out of the existing Health data available with IIB and
- supervised learning over a period of time based on the frauds established by the Fraud analytics system

shall be employed.

Bidder needs to specify and deploy the techniques like clustering, self-organizing maps, association rules, K-means clustering, expectation maximization, principal component analysis etc., which are employed for the unsupervised learning.

3.2.1. For the purpose of supervised learning, vendor needs to specify and deploy models like decision trees, Bayesian classifiers, nearest neighbor classifiers, support vector machines, neural networks, logistic regression, forecasting techniques, summary statistics, etc., which are employed. The emphasis would be to have country specific modeling approach that is based on the local experiences and needs. The solution needs to have anomaly detection capabilities and the Vendor needs to specify and deploy specific techniques such as outlier analysis, simple distribution based anomaly detection, Box-Whisker plots, clustering etc.

3.2.2. The solution should be capable of

a. using the knowledge generated through statistical and artificial intelligence tools /models,

b. performing processing based on the patterns of fraud mined from the

- existing data of history of claims/underwriting and also
- detect and prevent upcoming patterns

to identify the degree of suspiciousness in underwriting of proposals/claims through anomaly detection methods or any other relevant statistical and artificial intelligence models. This shall include hypothesis formation including gathering evidence, development, testing and improvement of fraud models.

3.2.3. The solution also needs to capture and encode experience-based knowledge related to fraud detection. The solution needs to build historical information and generalize from known historical examples of suspicious claims/declined cases. The generalized knowledge can then be used to classify new claims/proposals.

3.2.4. **Simulation:** The solution needs to have ability to build scenarios by using simulation tools. Capability shall be provided to expand to additional parameters' set in response to the changing needs by understanding how a policyholder/proposer behaves under abnormal (fraudulent) circumstances from past behaviors. This support shall be to supplement any product/underwriting rules deployed by the insurers at their own offices/systems.

3.2.5. Additionally each fraud/suspicion of fraud shall be categorized to indicate the degree of suspiciousness and for investigation/statistical/analytical purposes or management decision making.

3.2.6. Going beyond claims fraud detection, the solution needs to have prevention capabilities by deploying a framework, at policy inception i.e., underwriting, to prevent fraudsters from taking out policies in the first place and also at admission of claim before a claim is paid.

3.2.7. Real-time or near real-time support to decision-making of Insurers to prevent fraud before it happens shall also be provided.

3.2.8. **Clustering**: The solution shall have the capability to perform a cluster analysis by grouping objects of similar characteristics. Clustering is essentially required to explore further relationships between objects of similar characteristics and to draw conclusions. To enable the users to perform analytics manually, tools and visualization shall also be provided.

3.3. Scoring and Rule management:

The bidder shall deploy a suitable rule engine for the purposes of this project. The rule engine shall facilitate easy configuration of rules/models that are newly embedded. Further, rule engine shall provide ease of updation so that new rules/changes to the old rules can be carried out with ease. To achieve this purpose, the bidder shall also devise a strategy for rules management for

IRDA/IIB to consider. The following is the list of business requirements with respect to the scoring/rules:

3.3.1. The solution needs to have capability to score/rescore claims/proposals for insurance in real time-dynamic mode based on parameters, associated weights for risk scoring. The online scoring/rules engine needs to combine business rules, anomaly detection and other advanced analytic techniques. The vendor needs to specify and deploy the above techniques and others such as Association rules, Machine learning tools etc.

3.3.2. The solution needs to have capability to calculate the propensity for fraud at first notice of loss, then rescore claims at each settlement stage as new claims data is captured. Similarly, the scores shall be calculated at the time the proposal data is captured for the first time and every time it is updated with new information before a final underwriting decision is taken.

3.3.3. The solution should have capability to calculate risk scores based on specific characteristics of the activity including geographic zones etc.

3.3.4. The solution should support creation and management of business Rules for known fraud patterns and analytic models and logically manage rules, models and alerts for investigators. All rules shall be written by the bidder as authorized by IRDA/IIB from time to time. However, creation/updation of Models may also be done by IRDA/IIB users after 'GO-LIVE'.

3.4. Triggers/Alerts:

3.4.1. The solution shall establish triggers/alerts for early detection of the frauds/suspicious transactions and they shall be categorized to indicate situations that warrant special attention or further investigation at the level of Insurer or Intermediary.

3.4.2. The solution needs to have alert management capability to assemble alerts from multiple monitoring components and associate them with common claimants/proposers and give Insurers/Intermediaries a comprehensive perspective on the risk of specific claimants/proposers as the case may be.

3.4.3. The solution should have capability to prioritize alerts. The prioritization initially would be based on the parameters defined in the system. However, capability shall be provided to the user to re-prioritize based on insurer's own business rules/regulatory requirements. The alerts generated by the system shall be automatically assigned to the users and follow the workflow prescribed at the time of implementation. Capability to re-assign to a different team member shall also be provided. Complete transaction history shall be recorded with respect to the workflow of these alerts.

3.4.4. These triggers/alerts need to be in the form of on-screen pop-up messages, e-mails, dash-boards, dialog boxes, downloadable content, web-services messages etc.,

3.4.5. It may be noted that to transmit these messages, the cost related to the relay service (if any) shall be built into the total cost of the solution.

Indicative triggers for claims include but are not limited to the following:

3.4.6. **Policy and Claim history triggers:**

- Claims from a policy with only one member of a family at minimum sum insured amount or very high sum insured
- Multiple claims with repeated hospitalization, multiple claims towards the end of policy period, close proximity of claims etc.,
- Claims made immediately after an endorsement.
- Claims from a member with history of frequent change of insurer or gap in previous insurance policy.
- Claims for policy with evidence of significant over/under insurance as compared to insured's income/life style.
- Claims from members with no claim free years during the preceding three or more policy years.
- Small claims in huge numbers from the same hospital or for the same treatment etc

3.4.7. **Provider location or profile triggers:**

- Claims from a hospital located far away from insured's residence, pharmacy bills away from hospital/residence
- Claims for hospitalization at a hospital already identified on a "watch" list or "black listed" hospital.
- Claims with inconsistency in diagnosis and line of treatment. Inconsistency between specialization of treating doctor and illness etc.,

3.4.8. **Diagnosis triggers:**

- Claims for medical condition which is a potentially pre-existing disease being managed surgically/treated in the first year of the policy.
- Claims with unjustified use of advanced treatment procedures/facilities for a minor complexity.

3.4.9. **Billing triggers:**

- Claims with disproportionate pharmacy costs, surgical fee, hospital bill or doctor's fee.
- High value of claim from a relatively small hospital not known for an advanced treatment capability.

The bidder is expected to build master data and rules for a user configurable rules management application of the solution with respect to the identified trends/triggers as above.

3.5. Profiling:

The solution needs to have profiling functionality as stated below:

3.5.1. Employing statistical analysis and artificial intelligence techniques to profile proposers/claimants, other stakeholders (insured, providers including hospitals, doctors, intermediary or any agency/firm involved in the health care/medical insurance system) and products based on parameters underlying the behavior of each of these stakeholders and products/services is expected. Development and continuous updating of profiles of stakeholders and products/services is also required.

It may be noted in this context that an initial effort in compilation of hospitals master list is attempted by IIB. The details are available as downloadable content on Health Insurance Data section of IIB's website (www.iib.gov.in).

3.5.2. It is expected that fraud data model for the stakeholders shall be developed by the bidder as a pre-cursor to the profiling, predictive and analytics work. The categorizing of profiles on various parameters like type, nature of business, customer segments to whom they cater to, specialty area, geographical area, income levels, claims tendency, etc needs to be carried out.

3.5.3. The functionality shall include summarizing normal behaviors, anomalies/outliers as well as exceptions. The profiling includes ability to group stakeholders based on variety of criteria and patterns. It also includes capture of deviation from these behaviors leading to suspicious situations and historical trends. The profiling needs to be dynamic in nature to respond to changing/emerging fraud methods/tendencies.

3.5.4. In addition, profiling for disease specific treatment procedures, diagnostic reports vis-à-vis the treatment/diagnosis, acceptable thresholds for various treatments/test results etc., shall also be devised.

3.5.5. The profiling shall also bring to fore, the potential aggregate level insider fraudulent activity within an insurance company/TPA/intermediary/other stakeholders including any issue arising out of a failure in the internal control mechanism to enable IIB/IRDA to alert the entity/party concerned.

3.5.6. Profiling of patient records along with Provider based on a time period is also required to understand the trends within each specialty, diseases and associated treatment procedures.

3.6. Predictive and classification capabilities:

The indication of selection against the insurer/suspicious activity shall be provided to the Underwriters/Claims Mangers/Representatives as a part of the predictive capability so that the possibility of fraud is eliminated altogether or at least minimized. The solution shall at a minimum provide the following capabilities as a part of this requirement:

3.6.1. Capability to identify and assist the Insurers to handle application for insurance/claims/enrolment of health care providers/intermediaries/any other party to the transaction by indicating the possibility of a suspicious/fraudulent attempt.

3.6.2. To support the predictive capability, the classification techniques such as decision trees, logistic regression techniques, association rules, support vector machines, neural networks etc., shall be provided. The tool should have the capability to generate and report 'confusion matrix' and sensitivity (True positive rate), specificity (true negative rate) and false positive rates.

3.6.3. Identify and notify (both real time basis or otherwise to the users), the possible predictive and analytical alerts (for Fraud in the data)including but not limited to

- Over-billing (higher-than expected rates)
- Unusual changes in transactions or amounts over short periods of time
- Unusual changes in patient activity or health care profiles
- Unusual billing by hospitals or treatment patterns etc.,
- Excessive number of procedures
- Unwarranted procedures, excessive investigations, expensive medicines
- Over-utilization, extended length of stay at the hospital

3.6.4. Patient history

For effective fraud handling, every application that is being underwritten and every claim that is being processed shall in addition be provided all necessary information (both real time basis or otherwise). The support provided includes but not limited to the following:

- Summary information of the claims history of the persons/members being insured.
- Summary information with respect to a particular risk class
- Summary information with respect to the pre-existing diseases
- Summary information with respect to the Personal/Family History of the person/member being insured.
- Summary information giving the details pertaining to earlier rejection of a proposal/claim by a different insurer.
- Summary of profiles and scores.

- Summary information with respect to the claims, procedures, etc.,
- Summary information about the treatment cost for a stated disease/hospital category/geography or a combination of these factors.

3.6.5. Fraud history, details of suspicion etc.,

3.7. Link and Social network analytics:

The solution needs to store structured and unstructured data to build link and basic social network related analytics for understanding of relationships between behaviors and to find fraud rings and collusions using text analytics.

3.8. System Effectiveness:

It is expected that the Vendor comes up with a framework to improve the efficiency of statistical models and provide for suitable upgrades. Transactionally, the results also need to be cleaned up with appropriate discussion. The solution needs to have simulation techniques and the Vendor needs to specify and deploy techniques like Monte Carlo, Markov Chain, Boot strap, Genetic Algorithms etc. These techniques shall aim at reducing the false positives and false negatives. To monitor and achieve this purpose, the solution shall provide dashboards, periodic reports that indicate the effectiveness of the Fraud analytics system. In addition, the models devised shall be deployed only after a thorough testing so as to provide the desired level of confidence. This may be done via confusion matrix/matching matrix or any other suitable visualization methods such as Receiver operating characteristic curve (ROC), lift charts and cumulative lift charts etc. to measure the performance of the models being devised. Optimization techniques such as linear programming, sensitivity analysis may also be used for improving the results of the various models being deployed. The Vendor needs to specify and deploy specific techniques deployed for the purposes mentioned as above in this section.

3.9. Post Claims Analytics:

The solution should support identification, tracking and assisting Industry with intelligence on the possible trends/patterns/concentrations and development of statistical models, rule engines in drawing up of the trends. In addition, root cause analysis of various fraudulent/suspicious transactions shall be done on a periodic basis to narrate the trends and suggest areas of corrective action with respect to the suspicious/fraudulent activities. Output generated in this respect shall include but are not limited to the following:

3.9.1. Trends with respect to the stated category/across various categories of hospitals.

3.9.2. Trends with respect to a stated intermediary/across various intermediaries.

3.9.3. Trends with respect to treatment cost for a stated procedure, nursing charges, specialist fees etc.,

3.9.4. Trends with respect to type of claim payment (reimbursement/cashless/pre, post hospitalization, hospitalization) for indemnity policies.

3.9.5. Trends with respect to duration of the hospitalization, time taken to settle different capabilities:

3.9.6. Trends of overcharging or Unlawful claim (e.g., based on false data) or false claims or multiple claims for the same event in a particular region

3.9.7. Trends of Claims for pre-existing injuries or damage

3.9.8. Trends of Treatment not being commensurate with the disease

3.9.9. Trends of huge volumes of treatments in a single hospital in a stated city/region etc.

3.9.10. Trends with respect to the suspicious activities

3.9.11. Trends with respect to fraudulent activities

These trends are perceived to provide critical inputs for management decision making. As such, breakdown structure to drill down to a granular level should be provided with a user interface. Also, capability for regrouping of the parameters, addition/deletion of parameters shall be provided to the users. The access to these trends shall be based on the requisite authorization matching with the role of the user.

3.10. Summary tools:

User interfaces with requisite features shall be given to enable the users to perform analytics with the data available. The screens shall provide the summarized information with graphs and other visualization. Flexibility shall be provided to summarize data on the fly. Ability to group, re-group, drill down or extend and compare across/link various data sets shall be provided.

3.10.1. The solution needs to provide interfaces including graphical ones like visualization that let Insurers identify linkages among apparently unrelated claims and uncover relationships previously not known.

3.10.2. Summary Information shall provide the required enablement for decision making to the Underwriters and Claims Managers/Representatives of the Insurers/TPA's by various means that includes real time alerts, dashboards, online screens, visualization interface, downloadable content etc.

3.10.3. The tool shall also provide various summary statistics like mean, skewness, correlation, standard deviation etc., for analytics based on user needs.

3.10.4. The solution shall provide capability to summarize data to suit the business needs and aid not just in transaction level underwriting/claims decision making but also enable organizational

policy level/product level/strategic decision making using statistical techniques like decision trees, association rules, etc.

3.10.5. **Operational and strategic analytics for the Industry**: Similarly, the solution shall provide the capability to summarize data to perform and decipher operational and strategic analytics at various levels (Region/Industry/Product etc.,). This will be essential for any regulatory oversight/supervision/decision making and for Industry development purposes.

3.11. Knowledge database:

To reduce the dependence on the human experience for fraud detection, the solution needs to draw statistical patterns in history of claims/declined cases and create as well as automate data bases of knowledge and processes to ascertain the claims that should be investigated and claims that need not be investigated. The solution needs to come up with front-end screens for Insurers to identify patterns and learn from them. The tool should be able to combine in an optimal way, the decisions/alerts coming from the domain experts and the alerts made by the data-driven tools that are part of the solution. This strategy of combining human knowledge with data driven knowledge is expected to provide highly accurate results in pin-pointing the possible fraudulent transactions. As a part of the knowledge database, the following at the minimum shall be addressed

3.11.1. Creation and maintenance of Red Flag masters/database

3.11.2. Identification and maintenance of data related to Fraudulent/Suspicious Providers, Policy holders, Geographies, Networks, Intermediaries, categories of policies, categories of treatments etc.

3.11.3. Creation and maintenance of data related to known behavioral patterns and tolerance thresholds

3.11.4. Creation and maintenance of data related to root causes of frauds

3.11.5. Creation and maintenance of data of frauds reported by the Insurers that are identified outside this system.

3.11.6. Creation and maintenance of data related to external sources of fraud data.

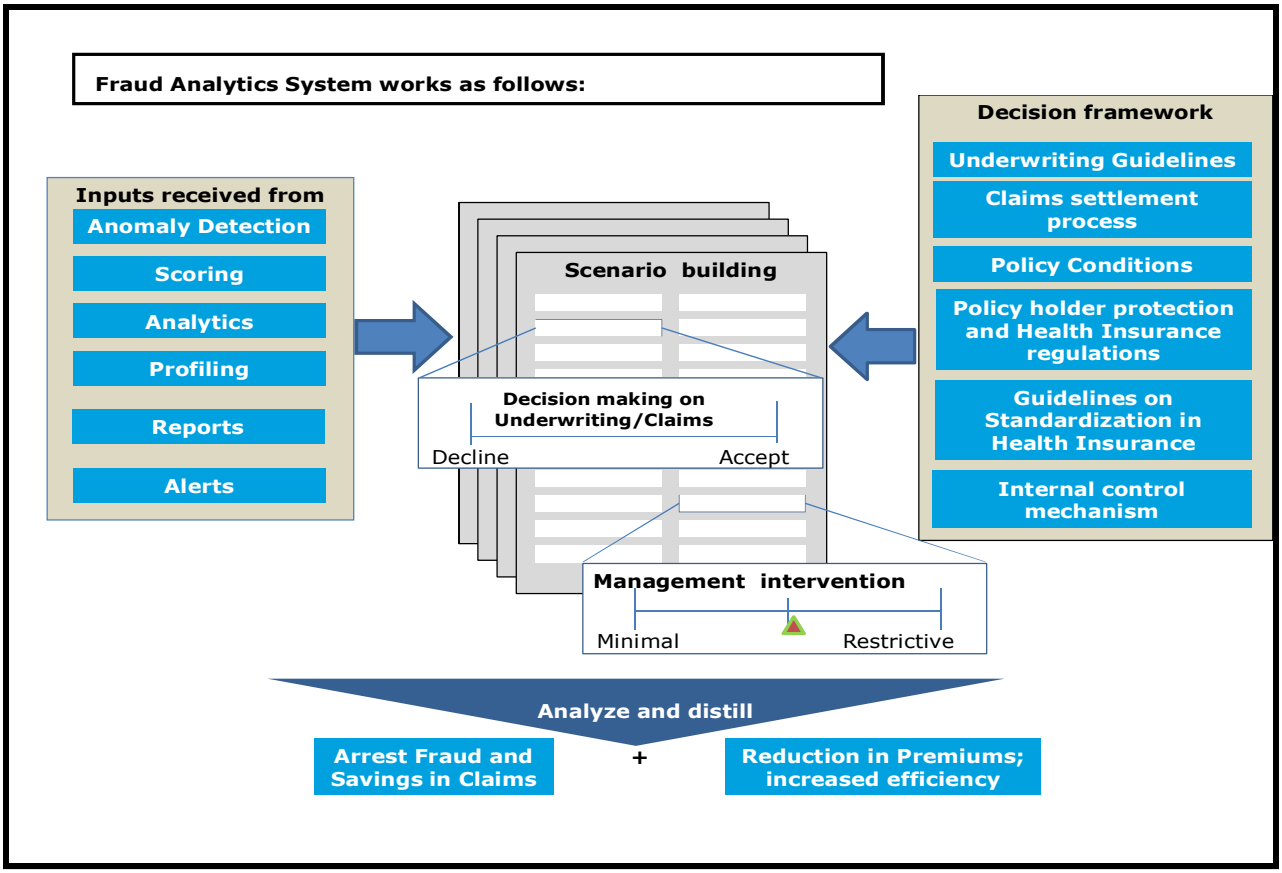
Section 4 :: Technical requirements

The technical requirements section broadly describes the requirements of IRDA /IIB. Besides laying down the technical expectations, this section enables the bidders to estimate the Hardware/Networking/Software components in establishing this system. This section broadly covers the Solution themes, Solution Architecture, Interfacing, Hosting, Sizing, Disaster Recovery, Security and other technical requirements. While, the broad intent is laid down in the following sections, the bidder shall primarily lay emphasis on looking to address the business requirements of the industry.

Executive summary of Technical requirements:

- Bidder shall be responsible for the acquisition and installation of the hardware/software/network and related components and shall be required to develop, operate and maintain the solution for the duration of the contract.
- The solution needs to be physically hosted at IIB and rest of Data centre related hosting including failover mechanisms, BCP and DR will be the responsibility of the Vendor
- While the RFP proposes a broad statement of the requirements, it shall be the responsibility of the bidder to bring their Fraud and analytics capabilities and consulting experience to the table with respect to both big picture and drilling down each of the requirements into further granular level and addressing each of them as per the expectation of the IRDA.
- IIB shall be the primary source of data for the project and owing to the various analytics that are proposed to be carried out, need for further data has to be addressed. While data availability is a constraint for any Fraud analytics Project, it is accepted that the Project needs to take off and be implemented with the available data to start with. And, in order to deliver low hanging fruits, during the phase 1, all possible analytics that are possible with the existing data shall be prioritized. Other requirements shall be addressed as a part of phase 2. It is expected that both the phases 1 and 2 shall be deployed into production within a period of 18 months from the date of award of the contract.
- In the current day world, IIB collates transaction level data from the insurers and stores the same on the present day IIB's Analytics Server. On a timely basis, this data is being analyzed and summarized in the form of public reports for the interested parties. The IIB's present day analytics server will continue to collate the date as per the present practice. However, the FAS will help with the analysis with respect to the Health Insurance Segment and shall also enable fraud detection and prevention.

- A diagrammatic representation of the proposed solution is as follows:



- Capability of real-time interfacing with the insurers is envisaged and alerts generated shall be handled through an automated workflow process until closure.

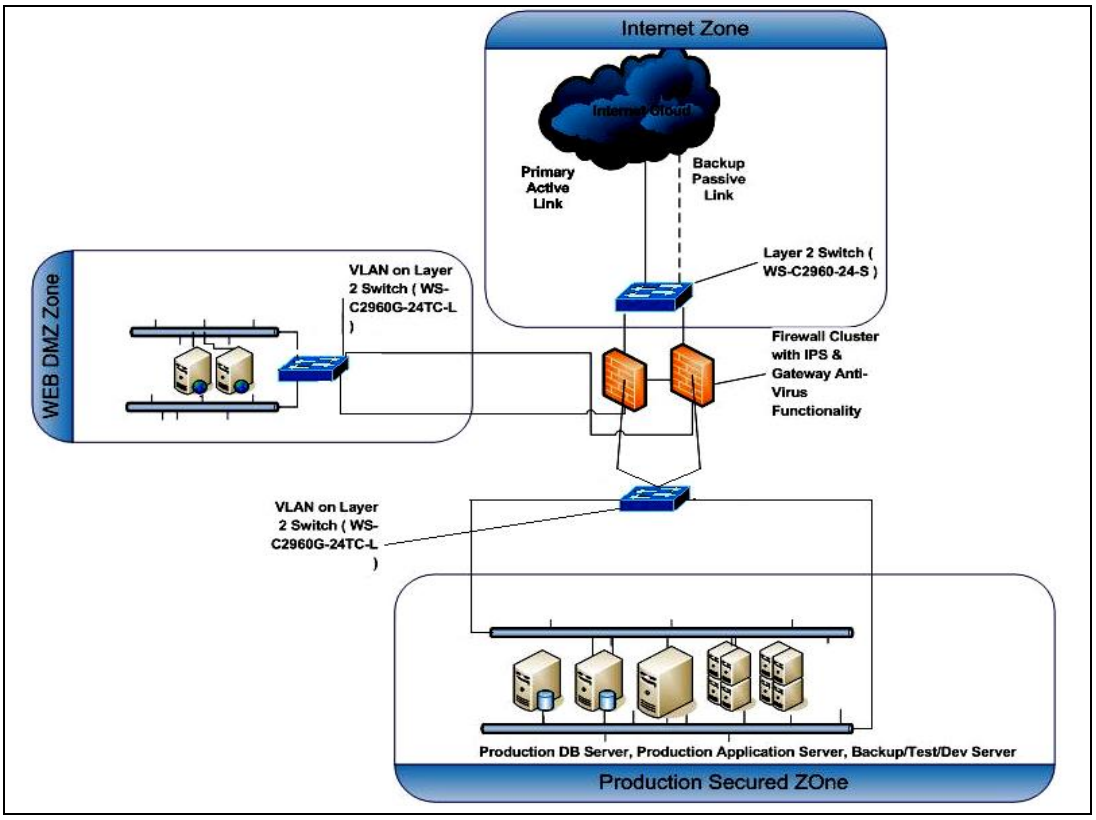
- DR is proposed as part of the solution and the Vendor needs to assist IIB to ensure that DR of the proposed solution needs to be part of the overall DR of IIB which may be put in place at a later date.

- The solution is accessed by the Insurance Industry, other Intermediaries & stakeholders and Regulators/IIB. Besides, the solution envisages the real time integration for decision making on proposals and claims. As such, the importance of security, availability and performance needs no emphasis. While boundary conditions have been given in the nature of architectural considerations and strategy for BCP/DR for Hardware/Network and solution sizing, the actual sizing and security strategies need to be conceived to address the requirements of the Project. The sizing needs to take into consideration performance parameters including envisaged response times, scalability, high availability, fault tolerance and load handling requirements as defined elsewhere in this document.

- The solution needs to conform to open standards in respect of hardware platforms and operating environment and inter-operability requirement.
- The solution needs to have a well laid out roadmap for scalability.
- The solution design shall support the extensibility to other lines of Business as envisaged by IRDA.
- As the Project is data intensive, the implementation agency is required to deploy appropriate data migration, quality and transformation tools to tone up data to align with the data as well as statistical model requirements of users in terms of context, aggregation levels and cleansing.
- The solution needs to conform to internationally accepted data standards in Insurance and health domain.
- Since the Insurance domain is process intensive, there is focus on unstructured data as also text mining. Thus the technical capability of the solution needs to cater to this specific requirement.

4.1. Existing IT infrastructure of IIB:

Network diagram of the present day IIB analytics server is as follows:



IIB's Web application details pertaining to the present day analytics server are as follows:

1	i. Hosting: Where the target application is hosted? ii. Whether accessible remotely from Internet? iii. URL of the application for Staging and/or Production Server.	i)Application is hosted at IRDA Datacenter ii)the application can be accessed from remotely iii) https://iib.gov.in (PRODUCTION)
2	Operating System (e.g. Windows2003, AIX, Solaris etc)	Redhat Linux
3	Web/Application Server with version (e.g. IIS 5.0, Apache, Tomcat etc.)	Apache ,WAS 7.0
4	Server side scripts(e.g. asp, jsp, php etc.)	Jsp's
5	Database at backend(Oracle, MS SQL, MySQL etc.)	Oracle 10g
6	Database access type(Read Only, Read/Write)	Read & Write access
7	Type of cryptography used for storage and transmission of data and credentials.	DES algorithm is used for storing and retrieving of user password.
8	Type of Authentication (Basic/Form Based/Certificate Based) used	SSL Certification is used for authentication
9	Total Size of the Website in MB and in no. of pages	Total size of project is 38.0 MB.
10	Integration capabilities	SMS and Web services
11	Data quality solutions	TCS product – Data clean
12	DR site	Currently no DR site is available. However, it is proposed to be set up soon.

Information security policy of IIB is available as Annexure 2 (File Name: Annexure 2_IIB_Security policy)

4.2. Solution Themes

The following themes of the envisaged solution are identified. These themes are the guiding factors in designing the envisaged solution.

Solution Theme	Description
Reduced manual intervention for fraud detection	This shall be the competency to automatically detect any fraudulent attempt/suspicious activity
Enhanced Analysis capability	The evolving analysis need of the authority to safeguard the Insured and Insurers and to support wholesome growth in the sector
Workflow and Notification	Managing the fraud alerts, follow-up action, corrective action, closure, etc on time

Information Dissemination	Share and distribute the information to various internal and external stakeholders with role base access control
Need based analysis	Through the online screens, the users will be able to perform various day-to-day analysis of the database and initiate effective management decisions.

4.3. Stakeholders of the envisioned System

The key stakeholders and their roles in the envisioned ecosystem are highlighted below

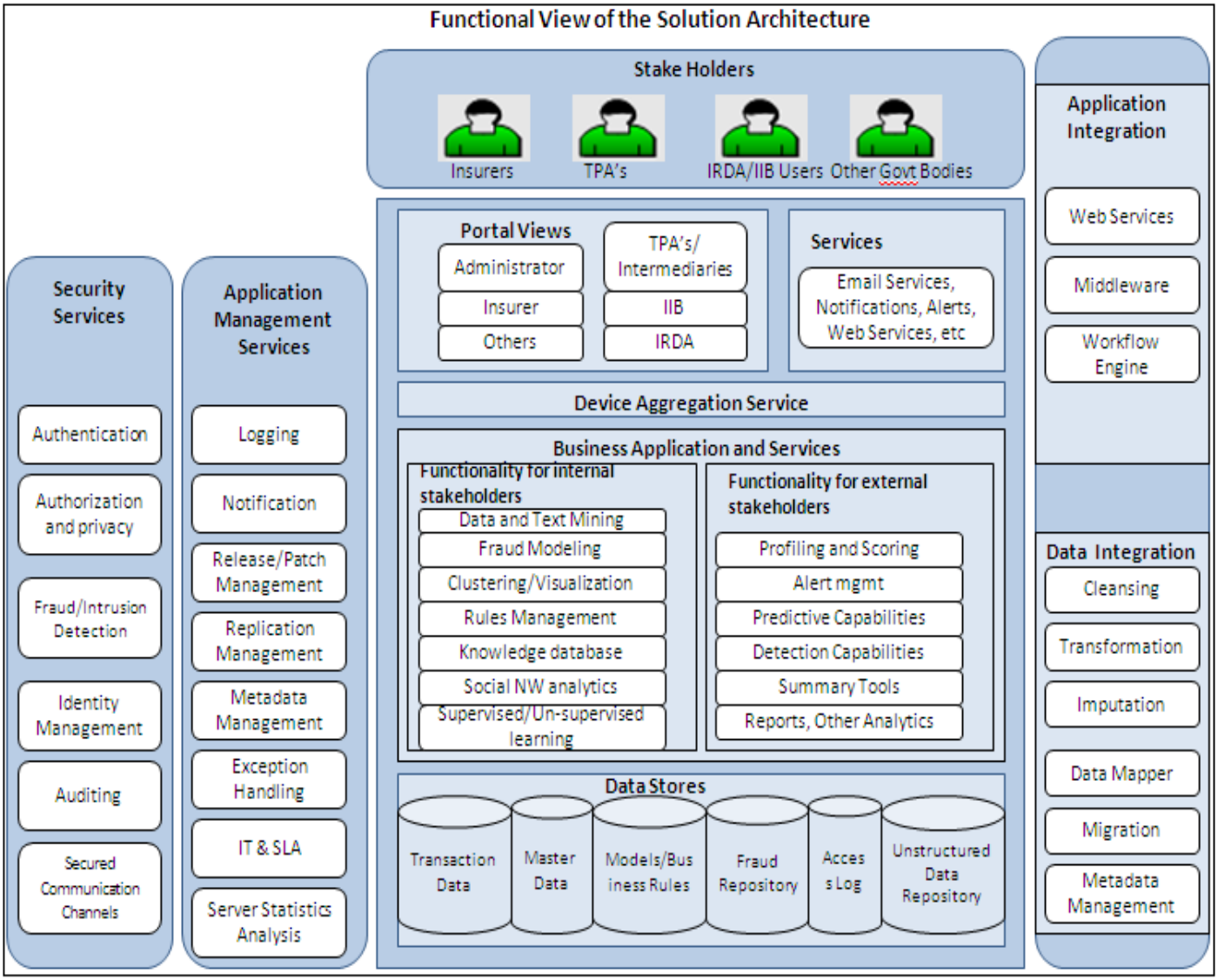
Stakeholder	Description	Role provided in the proposed system
IRDA	Generate analytics for regulatory decision making	Perform Analytics, Generate periodic/ad-hoc reports, Monitor the system performance, etc.
IIB	Analytics Support System	Perform Analytics, Generate periodic/ad-hoc reports, Monitor the system performance and operations, Build/alter models etc.,
Insurers	Use Analytics	Use Analytics for Underwriting/Claims decision making, record established frauds in the system, perform analytics for day to day business decision making.
TPA's	Use Analytics	Use analytics for decision making on claims and support the insurers in claims administration.
Other Government Agencies	Frauds Monitoring	Coordinate the efforts of monitoring the fraudsters across various domains.

4.4. Solution Architecture

4.4.1. **Functional view of the Solution Architecture**:

This view of the architecture elaborates various functional components of the envisaged solution. The functional components have been identified based on the functional requirements. Overall envisaged

technology platform of IRDA/IIB system will comprise of a set of applications and services that are expected to be rendered through a typical n-tier architecture configuration. A number of services will be hosted for internal consumption. A host of external services will also be rendered through this platform. Following diagram depicts the conceptual view of the overall services platforms:

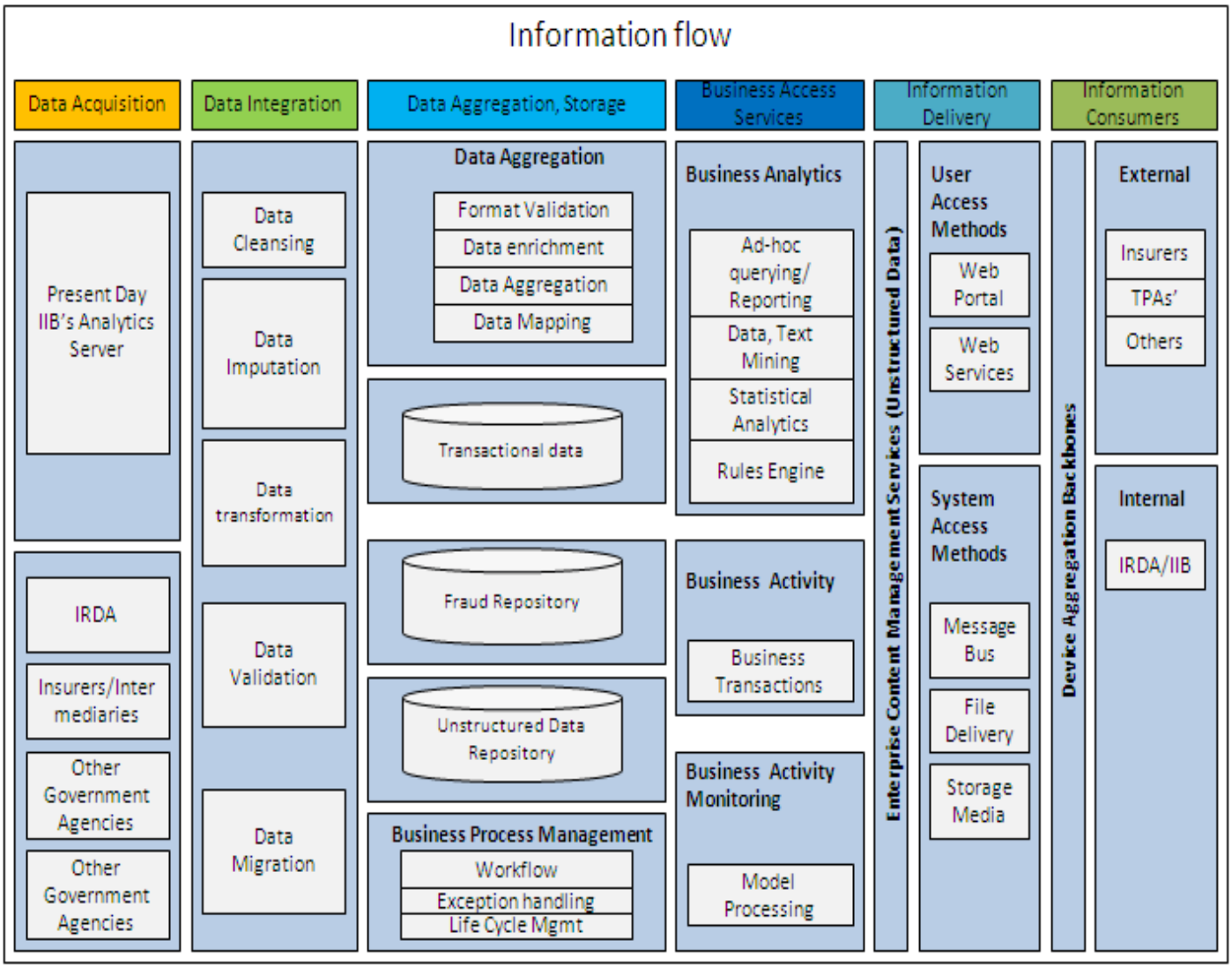


4.4.2. **Reference Architecture**: The following components of the solution architecture interact with each other:

- A front end user interface for performing analytics by all the users. Views that enable IRDA/IIB/Insurers to do various analytics for regulatory/management decision making
- A single repository of the Fraud
- Database of transaction level Health Insurance data that is migrated from the present day IIB server.
- Workflow system that enables manual/automatic processing at various stages of processing after a fraud is identified.

4.4.3. **Delivery Channel Architecture**:

This view of the architecture elaborates the flow of information right from its point of acquisition to its point of consumption by the various stakeholders. The information passes through various layers as following:



4.4.4. **Application/Services and Databases**

This layer includes:

- **Back End systems**: These are systems with which other business applications need to interact in uni/bi directional way with respect to information integration.

- **Core Infrastructure Services**: This would include all operational databases containing data pertaining to different business applications, users, user interfaces, metadata etc. It would also include communication components such as Email. The strategy with respect to the number, design and configuration of the databases shall be clearly drawn by the bidder as a part of the SRS and TDD documents and present the same for IRDA/IIB's approval. It is essential in this context to note that the strategy with respect to the databases shall be to primarily address the business requirements specified in the RFP.

Following are the key considerations for the envisaged solution:

- **Heterogeneous Environment**: Overall system is expected to have multiple components resident in different and diverse technology platforms. Proper consideration should be given to this point while finalizing the integration architecture.
- **End-to-end Integration (Data Level):** This application would have significant data level integration between legacy systems and the IRDA/IIB Portals which will pose a significant challenge in terms of latency, frequency of information. Ensuring the consistency and integration of transaction in a concerted mode will pose a significant challenge to this architecture

- **OS and System Software requirements**

  The system should be platform independent and should not only be deployable on multiple platforms such as HP UNIX, IBM AIX, IBM, Sun Solaris, Microsoft Windows, Linux etc., but should also allow integration with other software deployed across heterogeneous operating system platforms

4.5. Data centre and other hosting Requirements:

The solution shall be hosted by the bidder at the data center of the IIB at Hyderabad. It may be noted that IIB is contemplating at relocating to some other premises within the city of Hyderabad. IIB data center will consist of many applications and services which are delivered to the stakeholders and one of the applications is the fraud analytics solution. With reference to this solution, the requirement of the database environment, the application environment and the web environment is to be quoted by the bidder including the storage requirements. The products and services quoted by the bidder as a response to this RFP will require the complete implementation of the total solution by the bidder at the IIB primary data center. However, the space and support infrastructure required for proper functioning of IT resources deployed will be the responsibility of IIB. The IIB data center will have IT resources in addition to the resources that are deployed for meeting the requirements of this RFP as it has to cater to the requirements of other applications/services. **No part of the hosting shall be outsourced to any other agency.** IRDA/IIB shall have the visibility into the hosting arrangement from the official contract to monitoring of the hosting. IRDA/IIB shall have complete access to various reports, dashboards etc., related to the hosting, disaster recovery/business continuity arrangements. The bidder shall be responsible for the complete hosting solution, any issues arising out of such arrangements, adherence to the SLA's, data integrity and any other such issue.

It may be noted that the Fraud analytics system will be a standalone system and all licenses shall be obtained for enterprise level usage. No existing licenses/hardware can be leveraged.

The hosting arrangements shall at minimum meet the following criteria:

- State of the art hardware and tools for 24 X 7 monitoring. The bidder has to ensure that all the tools as well as software required to ensure complete administration, management and monitoring of the total solution architecture has to be a part of the offer in terms of delivering the expected services on an ongoing basis.

The man power deployed by the bidder round the clock for the above has to be competent, capable and more importantly have the relevant prior experience of handing such complex environments for other customers.

- **The configuration of the servers should be robust and capable of handling the load**.
- The server should have adequate storage capacity, configuration, speed, internet bandwidth and should have been directly connected to ISPs backbone providing adequate bandwidth and reliability with multiple links. **To support the requirements of this solution, a bandwidth of a minimum of 10 Mbps shall be provided.**
- At any point of time, the bandwidth capacity should not cross more than 70% of the provisioned bandwidth.
- The connectivity between primary and DR would be through MPLS and adequate capacity for the same may be proposed by the bidder.
- **Encryption layers (128 bit) shall be robust enough to ensure** complete protection of both, data and user credentials for the data in transit as well as in storage.
- **All data needs to reside within India and within the data center of IRDA/IIB.**
- The architecture should have **no single point of failure** and therefore the bidders have to ensure that, in the event of failure of any component or sub-system or software the resultant architecture is able to perform without human intervention and performance degradation. There should not be any compromise to data and transaction integrity in the event of failure of the above.

The bidder shall devise a **framework for security at the data center and at a minimum shall include Firewalls, IDS, IPS, Antivirus, Anti spamming and regular security audits**. The first point of authentication should happen in a demilitarized zone.

The Physical infrastructure for the Data center shall be provided by IIB. This includes Civil interiors, Civil and Masonry, Joinery, Access flooring and insulation work, False ceiling, Painting and Epoxy works, Access Control systems, Fire Detection systems, Air Conditioning systems and Power Back-up systems. However, the following shall be the responsibility of the bidder:

Electrical Works & Cabling and Racks:

- Power requirements including power outlets, wiring, cabling for network and power, racks, etc., shall be appropriately sized and provided by the Implementation agency. The power equipment and racks should have enough provisioning for redundancy and should be expandable in case of need.

The key considerations for ensuring high efficiency of Data Center (DC) operations are discussed in the table below:

Operations	Should be 24 x 7 x 365
Computing, Storage and Application Environment	From an operational perspective, the system should provide enough availability to give comfort to applicants in terms of reliability and efficiency of the system. Service Level for ensuring **uptime should be 99.5 per cent** The architecture should have **'No Single Point Of Failures'**
Communication Network	The MPLS backbone and Network should have assured uptime and therefore two separate links from two individual service providers should be used. Service Level for ensuring uptime should be 99.5 per cent
Information Security	Information Security at various layers prohibiting the possible security threats should be ensured. Security should be ensured for the application data, Network and Physical Infrastructure being set up under this project. Security threats from unknown networks integrating with IRDA/IIB such as Insurer/Intermediaries/External bodies need special attention and the design should take care of such users in a different manner.
Maintainability	Adequate spares at the sites for all elements with single point of failure, sufficient on-site manpower to failure resolution on site, and back-to-back spare replenishment plan with minimum spares turnaround time from the Product OEMs should be ensured.
Manageability	Latest tools for Incident Management including Help desk, Problem Management and Asset Management should be used and processes should be defined based on the ITIL framework.
Training	IIB's technical resources need to be trained to manage the data center for this project over a period of time

4.6. Solution Sizing:

The bidder shall provide various licenses to support IRDA/IIB's requirement under different categories as mentioned below. For the purpose of sizing the solution, the bidder has to take into account that the **resource requirement based on the number of concurrent users not exceeding 70% of the stipulated parameters**. The bidder will provide a comprehensive solution sizing, based on the information provided

by IRDA/IIB. The sizing estimate must include detailed server configuration, network architecture, platform to be used, data storage scheme based on number and type of users, IRDA/IIB's expected service levels as indicated in the SLA section of this RFP, desired response time, etc., and all underlying assumptions in arriving at the solution sizing. The solution should be scalable both horizontally and vertically without redesign. The SLA's regarding the high-availability and performance would be as per the Service Level Agreement section of this document.

The following would be the categories of the users of the proposed application initially:

- **Low weight Users** – These are users who will access the summary level information. Users in this category will perform the activity like send alert notification, search for pre-existing diseases/coverages or functions that enable them to underwrite or process a claim. An insurance company, Intermediaries and TPA's comes under light weight category and constitute not more than 70% of the total concurrent users.

- **Medium weight Users** – These users belong to IRDA/IIB's middle management who will perform the analysis on data and generate the reports. These users constitute not more than 10% of the total concurrent users.

- **High weight Users** – These users are power users either belongs to the top management or administrators. These users will perform analysis, assign workflow, view dashboard, navigating KM content, create new reports, graphs, trends, metadata etc. These users perform heavy activity on system for the purposes of management decision making and constitute not more than 20% of the total concurrent users.

S.No.	Particulars	Approximate No. of Users
1	Insurers	1000 Users
2	IRDA/IIB Internal Users	50 Users
3	Peer Regulators, Govt. bodies and others	50 Users
4	TPA's	500 Users

4.6.1. **Hardware sizing:**

A total of over 83 lakhs health insurance policies with 24 crores members during 2011-12 and 69 lakh policies with 25 crores members were issued during 2010-11. The Health segment is growing at the rate of 31% CAGR for the past 10 years.

It shall be the endeavor of the bidder to primarily address the sizing from the perspective of providing the predictive and analytical capabilities for the Health Insurance segment. The following broad principles shall be adhered with respect to the hardware sizing:

- The bidder shall finalize and procure the hardware and network capability requirement in order to meet the performance requirement as specified under Service Level Agreement section, technical requirement including acceptance test / quality control parameters for tender document.

The sizing shall be robust enough to handle the business processes, front end tools, analytics and searches on the knowledge repositories and various other databases. In arriving at the sizing, the bidder may consider all relevant sizing approaches and shall address the expectations of IRDA/IIB as laid in the functional and technical requirements of the RFP. The hardware/solution sizing shall also address the requirement of growth of usage of the solution for the entire duration of the contract. It is expected that a detailed document addressing the above points on sizing needs to be submitted as an annexure to Technical bid.

The specifications should be provided for development, quality & production servers, storage and others as required including RDBMS and other applications suggested as an overall solution as per the project timeline set in. In addition, a well laid out approach and roadmap for hardware enhancements shall be devised.

The existing Health insurance database shall be shared for replication on the solution's standalone database. It may be noted that the current size of the database with respect to Health insurance business with IIB is around 55 GB. The incremental annual data may be around 11 GB (going by the current data volume, but may depend on the data needs for the solution). The storage device sizing of 5 TB is assumed to cater to the needs arising during the contract period (which is five years from the date of phase 2 'GO LIVE'). However, owing to the increased volume of business over what is estimated now, if the storage resource utilization crosses 70% of its capability, additional support with due approval may be provided at a cost borne by IRDA/IIB. Though IRDA/IIB plans to extend this solution for the other lines of business, for the purpose of hardware sizing of this project, the bidder shall consider the requirements only of the Health insurance business handled by both the Life and Non-life insurers. For the purpose of sizing, the concurrent users accessing the reporting system for standard set of reports may be assumed to be 150 and those performing ad-hoc queries may be assumed to be around 50.

For any further dependency on estimation/sizing, bidders may refer to the Annual reports section of the IRDA's website for the relevant information.

4.6.2. **Hardware specifications:**

Based on the functional and other technical requirements, the bidder will need to propose an appropriate specification of the Hardware. In devising the configuration for these components, the bidder shall address the objectives stated below:

Sizing Objectives:

- High Availability: As stated in the 'high availability' section of the RFP.
- Separate Storage: Additional space requirements for IRDA in future will be ensured through a separate Storage Area Network (SAN) driven disk. The disk will also be mirrored to ensure data protection and integrity
- **Redundancy: Adequate processing and capacity redundancy have to be built in within the system to ensure zero to minimal disruption in the overall operations**
- There should also be free slots in the proposed solution for upgrading the RAM, CPU (in case of blade chassis) in case of immediate requirement.
- At any point of time, the total resource utilization should not cross more than 70% of the provisioned bandwidth.

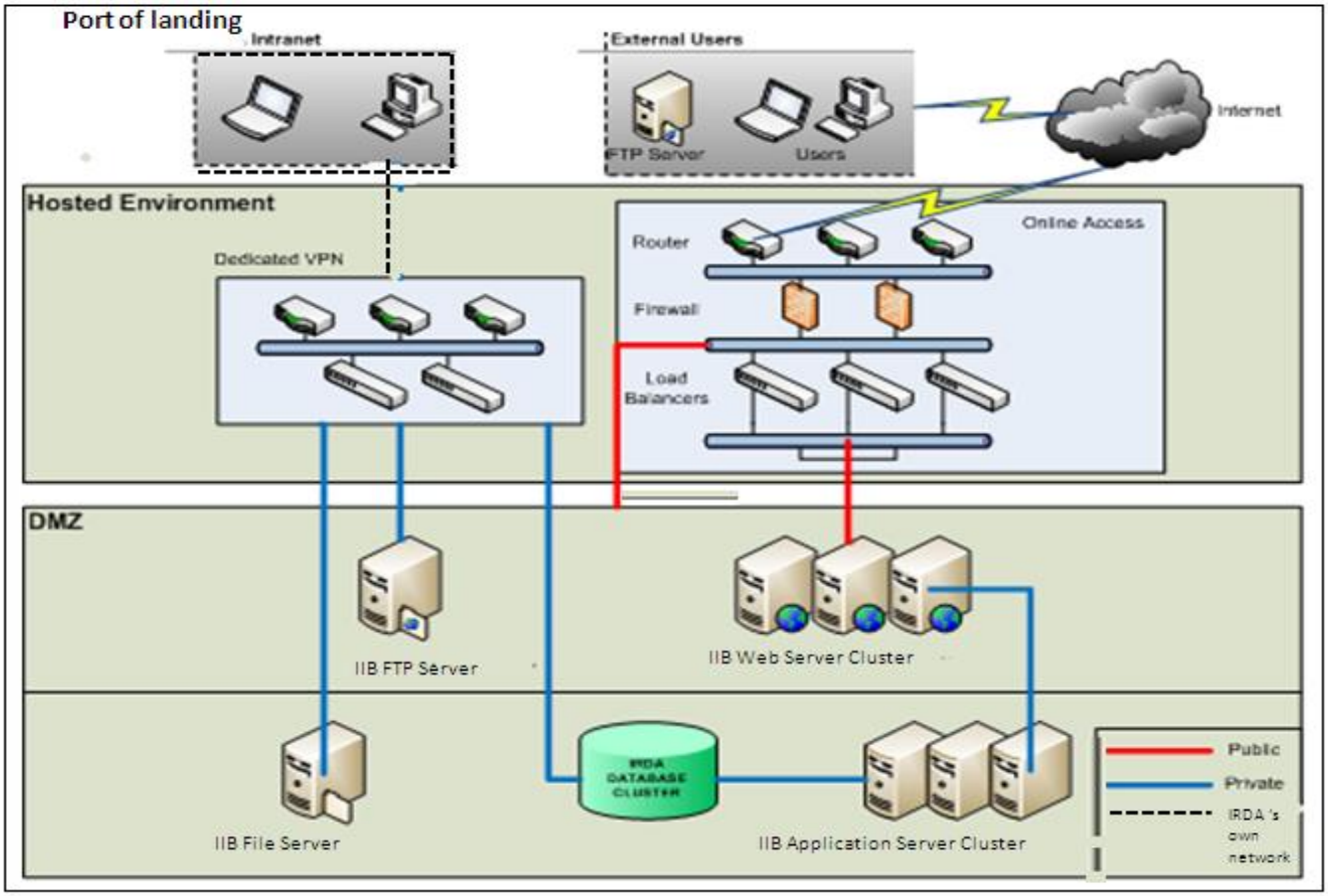
4.6.3. Architecture Considerations and Constraints

- The hardware sized for all the applications should be redundant and scalable. All the components within the server should be hot swappable and should incur no downtime due to component failure.
- All servers should have at a minimum of dual 1000 Mbps network interface cards (NIC) installed on different slots. Each NIC will be cabled from a different module on the switch using gigabit speed cabling.
- The system should have the capability to use Service Oriented Architecture best practices and should use industry standards for integration to achieve universal use.
- **The system should be database independent** and should allow deployment on multiple RDBMS such as DB2, Oracle, and Microsoft etc. The system should allow integration with other heterogeneous databases irrespective of the choice of database for the enterprise system. The database language should be ANSI SQL and should avoid using any Vendor specific proprietary extensions to ANSI SQL (e.g. PL-SQL)
- Ability to be browser independent. The system should be compatible with the following browsers
    - Internet Explorer 6.0 or higher
    - Mozilla Firefox 3.0.7 or higher
    - Safari, Netscape, etc.
- The system should have modular structure providing the flexibility to deploy selected modules as per the IRDA/IIB's convenience
- The system should provide fast and steady response times (Quality of Service). The speed and efficiency of the system should not be affected with growing volumes, especially during search operations, retrieval, archiving, reporting, MIS, knowledge management related activities under both online processes and batch processes.
- The system should be operational with good response time using low band width in the region of about 15Kb per user, especially for WAN and internet users.
- The system should meet the following scalability requirements:

- Support multi- tier architecture (The Application should at least have the following within its architecture) for all modules within the application with well defined interfaces between the layers
    - Presentation Layer
    - Business Logic Tier
    - Data Tier
- Capability to integrate with external / third party components like Rules Engine, Functional Modules etc which should not be point to point integration, but with well defined interfaces for data integration using enterprise data model
- Ability to scale horizontally without redesign
- Multiple similar hardware and mix of multiple hardware in a horizontal setup.
- Scalability for external components (External components should not restrict scalability) - Provide performance benchmarks for similar functions required in IRDA/IIB for Solution scalability
- Ability to scale vertically without redesign
- Addition of CPU, Memory, Hard disk capacity without causing downtime
- Support the deployment of additional modules at a later point in time with minimal downtime and loss of productivity.
- Support message patterns and protocols supported - e.g. publish/subscribe, synchronous/asynchronous, push/pull/pool, topics/queues.

4.6.4. Network Specifications

Networking will be enabled by two virtualized ports configured in a failover mode. Dedicated VPN links will be established between Development environment and Hosted Services environment for development purposes. The following picture describes the broad network architecture for the project.



Application design will ensure that all the data intensive processing will be restricted as back-end server process within the data centre environment. Data centre will operate on a dedicated 10/100/1000 MBPS LAN ensuring the processing integrity. All the master data managed facilities; application intensive processing as well as transactions will be carried out through the standard internet traffic from the field.

At this point of time, an overall network bandwidth of 10 Mbps is envisaged for running the operations efficiently. The responsibility of setting up of bandwidth shall be on the bidder. **Whenever the bandwidth utilization exceeds 70% of the capacity, additional bandwidth duly approved by IRDA/IIB shall be provided by the vendor at a cost to the IRDA/IIB.**

4.7. Performance Parameters:

The performance parameters are broadly defined in Service Level Agreement section of this document. The successful demonstration of the performance, scalability, load and stress testing shall be the basis for a GO/NO-GO decision by IRDA/IIB. In addition, performance evaluation tests (including scalability, load and stress) shall be conducted at periodic intervals as mutually agreed at the time of the contract. Any failure on these tests shall be subjected to the exit clause of the SLA and might also lead to

termination of the contract as per the provisions of the agreement entered at the time of award of the contract

4.8. Scalability :

The solution should be capable of scaling up for increased volumes for the period of contract as demands are expected to increase. The increase in demand will be both in terms of actual load and future functionality needs to be factored in for solution sizing, hardware sizing and also for planning performance of Solution, Database, Applications and Network environments. It is essential for the bidder to ensure that the compatibility and scalability of the software with the hardware and the existing assets in order to avoid issues of platform dependency and future capacity building. The entire stack of hardware/software/middleware stack shall fully address this requirement.

From an Operations perspective, the following best practices at the minimum would be followed to ensure scalability.

- Regular database re indexing
- Well-defined database maintenance plans
- Well-defined maintenance plans for servers
- Diagnostic tuning of servers to ensure best performance
- Quick Failure Isolation and replacement of faulty components
- Periodically measure the system performance counters of the server using System Management Console to ensure that the hardware is scaling up
- Disable unnecessary heavy performance logging in the system. (e.g. Windows PerfMon)
- Defragment the storage periodically
- Check the storage health periodically

From an Infrastructure perspective, the following best practices at the minimum would be followed to ensure scalability.

- High Availability: As stated in the high-availability section of the RFP.
- Redundancy: Adequate processing and capacity redundancy need to be built in within the system to ensure zero to minimal disruption in the overall operations
- Optimal network design to ensure best bandwidth usages
- Consider the use of Web Gardening
- Ideal recycle times for the Web Server process. Ensure that it is set to be recycled based on the resource utilization.

It is mandatory that the proposal indicates the scalability in terms of volumes specifying time and resources that would be required to extend the solution as demands increase. The increase in demand will be both in terms of actual load and future functionality. It is mandatory that the proposal clearly indicates the upper limit on capacities and features as well as the limitations of the solution in terms of number of simultaneous users, etc. It is mandatory that the proposed solution should be able to seamlessly communicate with the existing Insurers' systems, including hardware, system, application software etc.

Scalability should broadly ensure that the hardware and software chosen for the project do not in any way restrict or cause a constraint for a future requirement. It is also important that scalability addresses the load balancing and clustering of multiple environments/servers in multiple regions.

4.9. High Availability:

The bidder shall ensure that the high-availability, system uptime shall be a minimum of 99.5% for 24 hours a day and 7 days a week worked on a monthly basis with mean time to restore (MTTR) for the primary data center as well as the disaster recovery center independently. In any case, there should not be any data loss during the disaster recovery process. The bidder shall ensure complete access for IRDA/IIB to the remote DR for inspection or for any matter related to the general governance of the system.

Functional Area	**Required RPO**	**RTO**
Underwriting, Predictive Analytics	Less than 30 minutes	4 hours
Claims, Post Claims Analytics	Less than 1 hour	8 hours
Reporting and all others	Less than 4 hours	8 hours

Remote DR shall be stationed at a location that is in a different seismic zone. To ensure undisturbed connection between Data Centre and remote DR site the connectivity needs to be at least from two individual ISPs, one is for main network connection and the other is as fall back option. Similarly in DR site, internet connectivity should be same like DC. It may however be noted that the city of Hyderabad currently has only one power source. As such, suitable external data back-up, will also be required.

The solution while addressing the requirements for hardware sizing and scalability shall ensure that the Application, Web, database and other servers need to be designed in failover and firm mode with an ability to ensure full-proof operations.

4.10. Fault tolerance

BCP (Business Continuity Planning) will address the following types of failure LEVEL 0	
Failure	**Solution**
Failure of a component in a machine (Machine can be Network Infrastructure Devices and Servers and High-end user's Systems)	• Each machine should have 100 per cent fault tolerance capability. Fault Tolerance feature should be restored immediately

	• The faulty component should be replaced with a new component and it should be sent for repair/warranty replacement, etc at the earliest.
LEVEL 1	
Failure where the machine comes to a halt (Machine refer to Network Infrastructure Devices and Servers and High-end user's Systems)	• Each machine should have a backup counterpart. • During problem/breakdown of a machine, backup machine should automatically take over the job of primary machine • The faulty machine should be replaced with the new machine, which should be sent for repair/warranty replacement etc.
LEVEL 2	
Failure which causes the complete site to halt	• Two similar sites (one DC and one DR site) have been proposed which should always be up and running for normal operation. In case of higher recovery normal expectations a near site is also proposed which will get replicated at almost at a near real time. • In case of problem/breakdown of a site, DR should automatically take over the entire load and should start functioning as the primary site. • The status of faulty site shall be restored to normal as soon as possible
LEVEL 3	

Failure which causes the entire site to halt, including DR site	• Options such as hiring data center services from ISP vendors, etc. should be explored and latest backup should be restored to start the operation. • Efforts should be made to restore the normal status of DC and DR sites at the earliest

4.11. Access, Security:

4.11.1. **User Management/Access Control**: The solution shall provide facility to administer users including providing/denying access, assist users on issues related to passwords etc. Assignment of the access shall be based on the role of the user (Underwriters, Claims handlers, etc.,) and his/her level. The grant of access to various screens/part of the screens and capability to use shall also be driven by the purpose and role of the user as also the prevailing stage at which the work lies in the workflow. The super admin role would be with IRDA/IIB and shall have the privileges over the complete system. IRDA/IIB shall also have the capability to provide/deny/suspend/un-suspend/block role based access to authorized users within the Authority and outside. It may be noted that the IRDA/IIB users will access only through own network and outside users over the internet/IIB's web portal. Ability to configure and restrict the number of users for a stated entity shall also be provided to the super admin role of the IRDA/IIB.

4.11.2. **System Security:** The solution shall provide adequate framework for access by authentication, fraud detection, identity management, secured communication channels and auditing. The security system shall address the security requirements pertaining to the Application, System and Network.

	System & Information Integrity	**Identification & Authentication**	**Access Control**	**Audit & Accountability**	**System & Communication Protection**
Application	Application Integrity	Two - Factor Authentication	Role Based Access	Audit Logging	128 bit encryption
System	Software Integrity	Strong Passwords	Role Based Access	Audit Logging	Firewall HIDS/NIDS

		Identity Management			
Network	Two - Factor Authentication	Access Control Lists(ACL's)	Audit Logging	Two - Factor Authentication	ACLS

It is recommended that there will be two routers for the two different ISPs which will run in HSRP (Hot Standby Routing Protocol) mode. Since there is an interface with several external systems, adequate security layers with encryption will have to be built in. NIDS (Network Intrusion Detection System) should be installed to monitor network activity to identify any malicious threat. NIDS will centrally monitor the traffic that is coming in and going out from IRDA network. All traffic should pass through IPS (Intrusion Protection System) and then through the firewall for filtration purpose. The system shall also have the capability to notify the administrator of fraudulent attempts (successful and failed, both) to break into the system. Beyond the firewall section there should be two zones namely Demilitarized (DMZ) zone and Internet zone.

In DMZ there will be Web Mail server, Web filter server, Proxy server etc. For a Demilitarized Zone (DMZ), the normal access control should allow traffic to flow from the internet to the DMZ and then to the internal network, but should never allow anything to flow directly from the Internet to the internal network.

In the Internet Zone, there will be two firewalls in HSRP mode and data will be filtered and travel through these firewalls. This firewall will protect following zones:

Application Server Zone: All the application related server and related storage server will reside in this zone

Admin Server Zone: A the administrative servers (like. ADS, DNS, Global Catalogue server, Mail server Storage for mail server, proxy server, Antivirus server etc) will reside in this zone

LAN Zone: Through LAN Zone all the IRDA/IIB users will be connected

Subsidiary Zone: Through the Subsidiary Zone, all the subsidiaries will be connected and data will be filtered through these firewalls

In all the critical servers HIDS (Host Intrusion Detection System) should be implemented. The complete framework with regard to the security, list of encryptions (with details of what is encrypted and level of encryptions) shall be properly documented by the bidder and approved by IRDA/IIB.

4.11.3. **Software Integrity:** The solution shall address the Software Integrity bearing mind the following objectives:

- The system shall ensure that the mandated operational and technical parameters are within the prescribed limits.

- The System shall ensure that it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- The system shall ensure complete assurance that under all conditions an IT system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity.

4.12. Standards:

IRDA/IIB requires a solution that conforms to open standards in respect of hardware platforms and operating environment. One of the important criteria is to ensure inter-operability of the fraud analytics solution with other solutions which are deployed/under deployment at IIB. To ensure that interoperability efforts are minimal, it is mandatory for the bidders to conform to internationally acceptable standards. However this does not override the IRDA/IIB's discretion in deciding the Standard at any time during the bidding process. If the proposed solution includes any proprietary components, the bidder should identify such components and also provide details about service availability in terms of support, upgrades, on-going maintenance and other such areas.

4.13. Interoperability:

Interoperability is essential for the solution. In order to apply Interoperability to the solution the following challenges may arise:

4.13.1. Technical interoperability:

Technical Interoperability covers the technical issues of computer systems. It includes issues on platforms and frameworks. Frameworks for the solution might become complex and many times provide conceptual differences to working approaches. In addition, at times frameworks are duplicative and contradicting with multiple levels. Hence, thorough review and utmost care should be taken while deciding on the frameworks and platforms for the solution. Some of the specific platform and framework related considerations for the solution are:

- Choice of the operating system for both client and server
- Option to use server farm and use load balancing to host the web based user interface.
- Choice of the browser and it's add on components
- While we envisage to have as comprehensive solution as possible, there is need to implement predictive modeling markup language (PMML) compatible data and text mining solutions using which the fraud detection models developed by the proposed solution can be interoperable/exportable to other tools/solutions should the need arise in future.

Other considerations which are dependent on the platform and frameworks are:

- Portlets built for one portal platform would not interoperate with other portal platforms

- Developers would need to build the same portlet many times to support multiple portal vendors.
- A limited number of portlets will be available from a particular portal vendor for page designers.
- Deployment of portlets may want to be managed on certain systems but "consumed" on other systems.

4.13.2. **Organizational interoperability:**

Organizational interoperability is concerned with organizational processes and cooperation of agencies. Some of the processes may not be enough flexible and adaptive to be integrated and be interoperable. The IRDA/IIB top level management will need to play a vital role in such a context. Leadership and strategic direction of management are cited as the most important factors for corporate adoption of Web technology.

4.13.3. **Semantic Interoperability:**

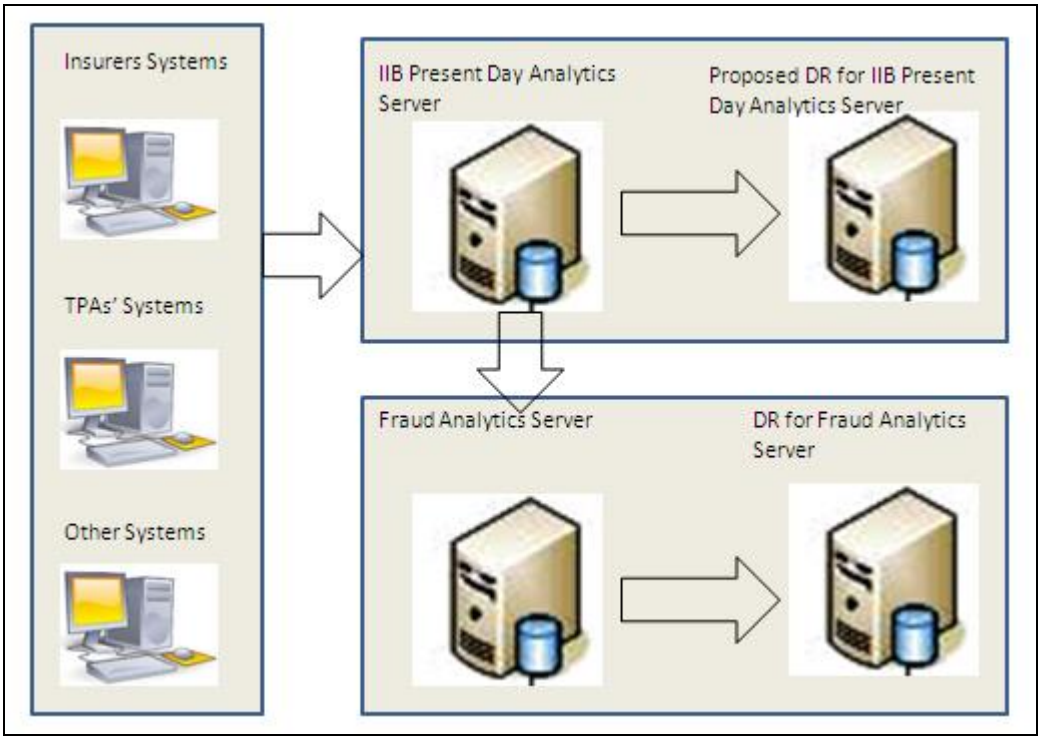
Interoperability or integration efforts are about making information from one system syntactically and semantically accessible to another system. Syntax problems involve format and structure. Semantics being an important technical issue is one that is almost invisible outside technical circles. What it boils down to is that the meaning of apparently identical terms can differ in significant ways between systems. Such differences normally make it more difficult to make systems work together. The differences can be minimized if systems are designed using agreed data formats. Semantics relate to the understanding and integrity of the information.

4.14. Interfacing:

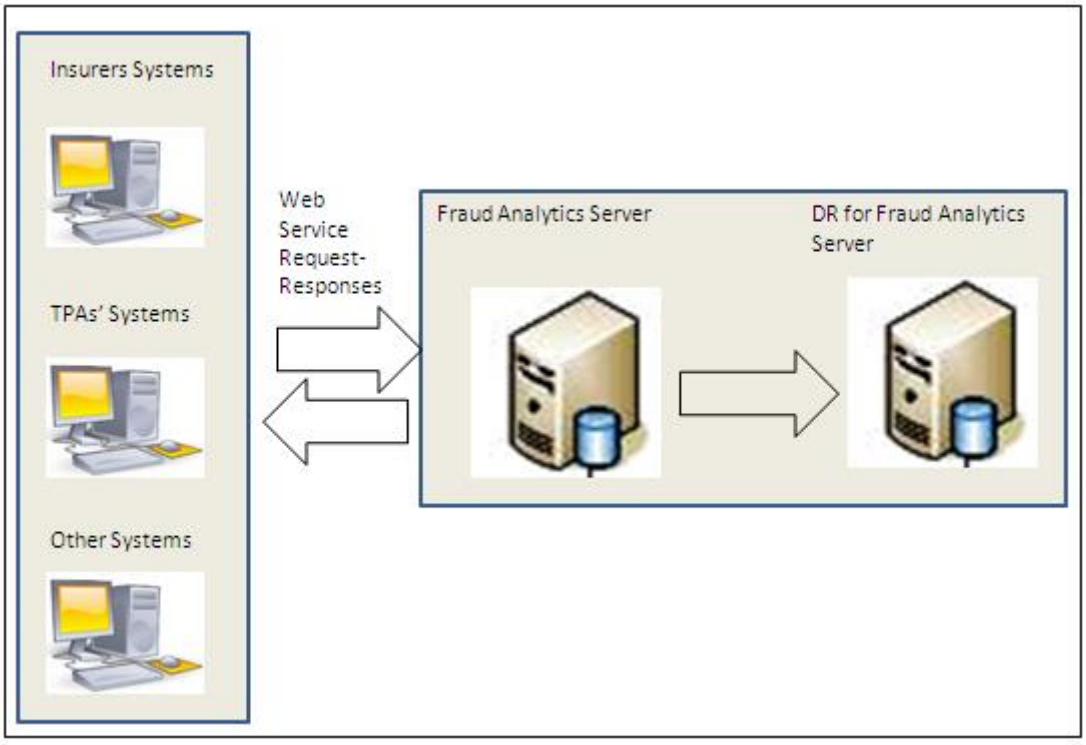
4.14.1. Introduction:

The present day IIB's analytics server receives and stores the transaction level data pertaining to several lines of business. This practice shall continue to be followed. The Fraud Analytics solution shall get a feed of the historical health database from the present day IIB's analytics database. In addition, it will also get a feed of newer transactions on a regular basis. The integration and interfacing requirement is to be built as a part of the solution architecture to meet the current as well as the future requirements to deliver the services as expected. For example: With respect to the insurers/TPA's, two-way interfacing should be possible to provide web services with security layers as and when required for accepting data in the defined format and providing return results in form of reports. Information that is relevant to probe the suspicion alert generated by the system shall be made available to the Insurers/TPA's.

An indicative diagrammatic presentation of the proposed interfacing requirement is as below: *Transaction level Data interface for the Fraud Analytics:*



Fraud Analytics related Query-Response interface:



4.14.2. **External interfacing:** The solution should support integration with suitable third-party databases. The aim of the project is currently to serve the needs of the insurance sector only. Any fraud related red flag masters shall be maintained within this project. But, due to growing awareness of fraud and various governmental agencies working on fraud area, interaction and exchange of information, ideas, methodologies can be expected. As such, the solution should be capable of consolidating historical data from internal and external sources (like CIBIL, declined card index database or other databases that may be provided by other regulators/government agencies) for fraud analysis and investigation both at the time of initial data migration and subsequently on an ongoing basis. The solution should also be capable of integrating with external applications/pre-packaged databases to the extent required and relevant.

4.14.3. **Integration with IIB's systems**: The solution needs to integrate with the existing IIB systems and adhere to the IT policy and architecture guidelines that IIB may have/stipulate.

The following is the indicative list of interfaces for this solution:

External:

Insurers
TPA's
Other Govt Bodies like CIBIL, etc.,

Internal:

IIB's Present day analytics system
IRDA's BAP system
IRDA/IIB's intranet
Sub-systems of the Fraud Analytics System like Workflow system, Rules engine, Data quality/imputation solutions etc.,

4.14.4. **Real time Integration with Insurers'/TPA's systems**: The project aims at empowering the underwriters and the claims personnel in taking informed decisions supported by the analytics and fraud indicators. This necessitates real time query and data exchange between the FAS system and the insurers/TPA's systems. The solution shall provide real time integration through web services between insurer's/TPA's systems and the fraud analytics system. This includes Integration with existing business processes e.g., on-line claim processing systems. It may be noted that where the IT maturity of the Insurer is low, they may be allowed to integrate with the proposed solution through batch mode as an exception to start with till they ramp up their internal systems. As such, apart from the real time integration, other modes of integration like batch processing etc., shall also be provided till the insurer/TPA is able to meet the real time integration requirements.

It may be clarified here that the real time integration shall mean the ability to receive a ''query'' from the Insurer's/TPA's system and to respond back with the response (both request and response through web services) with the purpose of enabling the underwriters and claims handlers in the process of decision making.

Within a real time response, all possible ''data and analytics'' that are relevant for an underwriting/claims decision making shall be made available. The bidder shall indicate the specific fields for a given response for IRDA/IIB to consider.

The system has to adhere to the real-time response times as indicated below:

- The real-time response time for an underwriting decision shall not exceed 10 seconds for a policy that is issued over the internet.
- The real-time response time for an underwriting decision shall not exceed 20 seconds for a policy that is underwritten at an insurer's office.

All other support shall be provided in a batch mode as follows:

- Response time for a pre-authorization check for cash-less hospitalization shall not exceed 15 minutes.
- Response time for other claims processing shall not exceed 2 hours.
- Any other batch response – 30 minutes.

The bidder is required to assist the IRDA/IIB in facilitating resolution of any issues arising out of integration with the insurer's systems.

4.14.5. **Interactive Nature of queries***:* Owing to the nature of business, the query to the Fraud Analytics System is assumed to be made only after all relevant data fields are entered completely by the Insurers/TPAs. And, interactive querying typically as done in web search solution might not be exactly relevant. As such, the response times indicated above are from the time last input is entered in the Insurer's/TPA's systems till the time a response is received by the Insurer's/TPA's system. It may be relevant to note that, the insurers typically issue a few categories of policies over the internet that typically do not have a need for an extensive underwriting. While enabling the online issuance of the policies, necessary enablement in terms of fraud and predictive analytics shall also be provided.

4.15. Specifications for the failover mechanism:

4.15.1. **Business Continuity and Disaster recovery**: The bidder shall be responsible for development and implementation of a comprehensive disaster recovery and business continuity plans and setting up of the remote DR in addition to primary project site. The setting up of the remote DR includes

all the infrastructure, network and middleware required for the purpose. Owing to the nature of the data that is being handled**, the disaster recovery shall not rely on a Cloud based technology.** The bidder shall not deploy remote DR at a site managed by a third party. The remote DR shall be a perfect replica of the primary data center solution architecture. However, the bidder shall be responsible for adherence of agreed SLA's and maintenance of these systems (including auxiliary systems, power/power back ups, cabling, middleware etc.,) and shall deploy own resources for their management. The security of these systems shall be the responsibility of the bidder. The bidder shall prepare an inventory of all the devices dedicated for the use exclusively by IRDA/IIB and those that are available for common use. In addition, details and methodology for partitioning of the resources available for common use shall be documented and provided to IRDA/IIB. The bidder shall all times be responsible for all the issues related to the upkeep of the systems including the infrastructure with respect to the remote DRs and shall provide IRDA/IIB the visibility into these arrangements on an on-going basis. The data integrity with respect to the enterprise data available at the primary data center is of paramount importance. As such, an online replication between the primary Data Center and remote DR is being envisaged. And, in order to ensure undisturbed connection between the Data center and the DR, the connectivity needs to be at least two individual ISPs, one is for main network connection and the other is as fall back option. Complete documentation with respect to the BCP/DR strategy shall be provided by the bidder.

4.15.2. **Considerations for Business Continuity Planning (BCP)**

- In the context of IT services, typically BCP relates to creating backups or having alternate mechanism for providing un-interrupted continuous services during a crisis. Adherence to the following list ensures that the BCP strategy works with utmost ease at the time of any contingency.
- The disaster recovery center should be exactly like the data center in storage capacity and should share standby for each other in case of failure, switching immediately in case of a failure. The performance level should not go below 80% in case of failure of either site.
- **During normal operations, both the DC and DR should be running in the —Ac□ve-Passive mode with an automatic load balancer between them, sharing 80 per cent of the full envisaged load.**
- Maximum time for a down site to recover should not be more than 24 hours.
- No data loss should be envisaged during failure including data in the transmission lines.
- A drill should be carried out randomly once in a quarter to test the BCP functionality.
- Bidders should be encouraged to suggest their own business continuity plan during tendering process. Evaluation of solution proposed by the vendors and SLAs proposed by them should be key parameters for evaluating the technical proposals.

The Business continuity plan for the present day IIB's analytics system is available as Annexure 1 (File Name: Annexure 1_BCP_IIB).

4.15.3. Strategy for Disaster Recovery (DR)

Disaster Recovery is a strategy used for providing alternate option to at least restore key operations in case problems at main sites. In the context of IT services, typically DR relates to creating backups or having alternate site for restoring the operations. Below is a matrix showing the different types of disaster recovery strategies applicable for the Fraud Analytics project along with their technical specifications:

Recovery Strategy	Technical Specifications
Data Replication	• SAN Replication between the Data Centers for critical data bases needed to meet accelerated RPO requirements (up to 2hours or less of lost data)
Dedicated DB Servers	• Deployment of Recovery Data Center Database Server Capacity to support the critical Data Bases
Dedicated Application Server Capacity for Critical Applications	• Procurement of additional virtualization capacity at the Recovery DC • Purchase of additional applications, middleware, and tool servers at the Recovery DC • CPU, Memory, and Logical Partition upgrades to existing development, test, and stage servers at the Recovery Data Center • Upgrade of the Recovery DC Operations (people and process) capabilities to support production requirements • Expansion of E-mail Infrastructure to support resiliency across the Data Centers
Enhancements to Reduce Recovery Time, Complexity, & Risk	• Wireless Network Deployment • Technology Services Tools Resiliency • BCP Security Access Changes
Tech Services Tools	• Make monitoring and support tools resilient or quickly available at the recovery data center

4.15.4. Technical Considerations for the DR

- Network connectivity and sufficient bandwidth will be needed between DC and DR; burstable bandwidth provisioning should be negotiated with WAN provider(s).
- System software should be used to synchronize platforms at production and recovery locations
- Dedicated equipment is required at the DR, but it could be used to provide testing or development during normal operations
- Automated provisioning/repurposing of test and development equipment for production/recovery purposes is a recommended capability
- Boot-from-SAN, Ignite or similar process should be used to reduce recovery time
- Regular, full-scale testing of the disaster recovery solution should be performed

- A distinct DR site should be created in the next seismic zone, designed as the backup (mirror) site to the main site. The DR site should deploy the entire application solution (current and latest version of the application builds, and all solution components).
- **The DR site should be invoked automatically when the production site fails to provide its services and it should ensure that it supports a degraded performance of at least 80 per cent of that prescribed for the primary site.**
- It should be ensured that data is replicated at the DR site at regular intervals
- Routine tests should be simulated to ensure that in case of an emergency, rollover to the DR site happens automatically without any service downtime.
- IRDA should run all services and transactions from the DR Site, at least once in a month, on a non-peak day to check its performance in case of an exigency and service provider (s) should perform DR drills monthly.
- In terms of storage requirements for the DRC, IRDA needs to implement some type of Information Lifecycle Management (ILM) approach. Data needs to be classified and placed on the appropriate class of storage. IRDA needs to implement a synchronous or asynchronous replication approach for critical data (e.g. SRDF, TrueCopy, PPRC, SnapMirror, etc.).

4.15.5. Server Side considerations for DR

- The servers should be designed in an "Active/Passive" strategy for the SAN replication.
- The servers located in the DC will continually replicate to the clustered servers in DR.
- All storage/database servers have matching model numbers, CPU and memory configurations. There are duplicate SAN with identical disk configurations on both sites
- Use of technologies to create and maintain standby databases
- Non-Production servers would be used to support Production during a disaster or extended outage
- As a part of the disaster recovery procedures, all non-production components/servers would be shutdown.
- The production Web and Application servers would be mounted on the non-production hardware from the mirrored copies. The production databases can be started from the standby databases or restored from a backup or mirrored copy depending on the disaster scenario.
- Server Cluster will deliver high-availability functionality. This will enable the applications to remain available in the case of a hardware; network or Operating System failure on one of the servers in the cluster group.
- These Server Clusters will be configured with cluster resources required by the FAS application. These resources include network names, IP addresses, application data, services, and disk drives. Once the Cluster resources are brought online it then begins processing client requests.

4.16. Solution roadmap:

The bidder shall indicate the road map for each of the solution stack obtained from OEM. And, care shall be taken to assure that the OEM warranty shall not be for a period of less than contract tenure

beginning from the date of phase-2 'GO LIVE'. The bidder shall devise and deliver a solution support roadmap that consists of end-to-end guides for solution porting or integrating functionality into the solution.

4.17. Extensibility:

The solution should be capable of extending the fraud analytics to all lines of business under Insurance though Health is planned initially. The solution needs to have functionality to similarly extend to other personal lines of Insurance Business like Motor at the minimum. Capability to extend to any other insurance operations besides underwriting and claims shall also be provided.

4.18. Data Migration/Collection:

The solution provider needs to primarily use the data available with IRDA/IIB or any other source as may be warranted and suggest other mechanisms to accumulate further information on characteristics of fraud by collecting necessary information about claims from Insurers.

4.18.1. The bidder shall primarily look at utilizing the existing historical database for predictive/analytical purposes.

4.18.2. Also, it is envisaged that the Fraud Analytics system shall receive the feed of transaction level data at regular intervals from the present day IIB's analytics server as per the prevailing practice and as per the formats prescribed by IRDA/IIB. As such, a migration tool to ensure migration of the existing data into the Fraud Analytics database shall be deployed by the bidder. The bidder is additionally and completely responsible for the migration of the data to the FAS. It is also expected that the bidder comes out with means to identify the suspected fraud items with respect to the historical database and utilize the same as they will act as the building blocks for further work.

4.18.3. The solution needs to have surveillance, monitoring and timely alert generation abilities as part of predictive capabilities. As such, the bidder shall perform an evaluation of the existing data formats. The bidder needs to undertake data analysis to identify data enrichment opportunities and additional data fields that are needed and suitable for predictive analytics need to be clearly indicated to IRDA/IIB for consideration.

4.19. Data quality:

4.19.1. The bidder shall suggest a data policy for collection, consolidation, de-duplication and handling data. The database architecture should support collection of raw data, grouping, consolidation and cleansing of the data (historical or otherwise) in order to facilitate meaningful and purposeful analysis.

4.19.2. **Data Transformation**: The solution should have data quality tools that can reduce or eliminate data inconsistencies or redundancies and should have native intelligence to support Indian Insurance environment. And, to handle issues with the data (historical or otherwise), the bidder is expected to deploy data imputation algorithms to replace/populate incorrect/missing values of the database.

4.19.3. The solution shall provide a framework to ensure entering/submission of quality data into/out of the system. This requires multi-level validations that will enable identification of exceptions/errors, categorization of errors/exceptions and resolution of the same during data submission and subsequent processing.

4.19.4. **Pre-processing**: The solution needs to have the capability to capture, organize, report and use data by segregating data, identifying contextual data and categorizing the same at various data aggregation levels based on the business need. This will enable the users in generating analytics by digging contextual data at appropriate level based on the need.

4.20. Data standards:

The data needs to comply with industry and other internationally accepted data standards and also ICD – 10 (International Statistical Classification of Diseases and Related Health Problems) or any other standard as may be required. In addition, the bidder may also refer to the "Guidelines on Standardization in Health Insurance" issued by the Authority and posted on the website of the Authority (www.irda.gov.in).

4.21. Data Structured and Unstructured:

The Fraud analytics system is expected to deliver various reports and analytics to its users. Fraud is an area that involves more analysis on unstructured data and fraud in insurance is more process intensive than transaction intensive. Bidders are required to scout for solution that addresses our specific need.

4.21.1. The solution needs to address not only transaction oriented fraud but also process oriented fraud and hence have capabilities of Fraud data management including the ability to perform structured data and unstructured data analysis by using big data analytical tools.

4.21.2. Intelligence shall be built to analyze unstructured data to suggest behavioral patterns, relate the outcome of analysis to a specific set of the stakeholders or flag a potential fraud or an emerging trend.

4.21.3. Matching of fields like PAN Number, Aadhar Number, Passport number, previous policy number, address of the insured etc., may be required to identify any previous undisclosed history of pre-existing disease or suspicious activity by the applicant/insured/claimant.

4.21.4. Additionally trends with respect to the pre-hospitalization/post-hospitalization/recovery procedures etc., may also be generated to empower the underwriters/claim representatives of the insurers to take informed decisions.

4.21.5. The solution shall establish a repository for the unstructured data to enable the performance of various analytics that are conceived as a part of this project.

4.22. Text mining:

4.22.1 The solution needs to have Text mining capabilities to analyze textual information in the claim such as the names, addresses, accident or treatment descriptions, general remarks of a claims handler etc., for the purposes of predicting/analyzing frauds.

4.22.2 The text mining shall aid in deriving patterns within data in respect of applicants for insurance/health care providers/intermediaries/insured/claims/treatments/treatment costs etc. These patterns shall be used both for understanding the trends as well as for detection/analysis of fraudulent behavior.

4.23. Data mining:

4.23.1 The solution needs to have data mining capabilities which may be used either to try to find (i) “rare” and “interesting” data records or (ii) groups of “similar” records or (iii) very common or very rare associations between records.

4.23.2 The techniques need to draw on the recent innovation in identifying interesting cases and also unbundling patterns.

4.24. Reporting:

4.24.1. The solution shall provide tools and technologies to generate standard set of periodic reports including dashboards and score cards. The Information consumers for reports and dashboards include IIB/IRDA, service providers and insurers and intermediaries such as brokers/agents/TPA's etc., The bidder is expected to bring the best practices as part of the solution for developing periodic reports and queries.

4.24.2. The solution should support the ability of IIB and/or IRDA to draw on the processed and/or under process data/analytics of the proposed solution for further analytics outside the scope of the proposed solution.

4.24.3. Analytics generated by the system shall be made available for the use of various users based on their roles and needs. As such, the system shall provide for the capability to report on all the analytics being generated. The structure and type of these reports, the frequency and the interested/target users list shall be based on the analytical algorithms being used by the solution and shall be submitted for a review by IRDA/IIB for finalization.

4.24.4. The solution shall be capable of generating reports that are essential for a regulatory review/decision making/IIB's use on various criteria including but not limited to the following:

a. Types of claims
b. Types of frauds/suspicious activity – cause wise, duration wise, perpetrator wise, amount of fraud, etc.,
c. Number/amount involved in claims
d. Monitoring progress on cases/transactions flagged as suspicious/fraudulent and subsequently closed, outstanding, under review etc.,
e. Cases established as fraud with details of amounts recovered or provided for.

4.24.5. The solution shall provide tools and technologies to generate customized/ad-hoc/on-demand reports. To enable generation of customized reports that meet specific needs of the users, screens with standard templates and with features like filtering, sorting, slicing and dicing, drilling down, export to word/excel, printing options, email options, drag and drop etc., which normally come with any standard reporting tool shall be provided. These features shall also be made available for the standard set of reports referred above.

4.24.6. Further, the solution shall also facilitate executing simple SQL queries by the users.

4.25. Workflow:

Every alert generated shall go through the workflow prescribed. Capability to handle the workflow with respect to the alerts generated beginning with assignment of unique identification numbers, identification and assignment to the users based on their authorization levels, follow up and tracking the same till their closure shall be provided by the system. Capability to review the performance of the users who are assigned these alerts based on several key parameters shall also be provided. The workflow system should provide the following functionality:

4.25.1. Assigning/re-assigning priorities
4.25.2. Capability to transfer work to a different user
4.25.3. Capability to monitor the status
4.25.4. Record the complete history of the work

4.26. Response Times/Load handling:

Loading, scalability and stress testing would be conducted prior to —Go-Live (phase 2), once the system testing and integration testing of the configured and customized solution has been conducted successfully. The stress and load testing requirements will be jointly determined with IRDA/IIB and the recommended testing tool will be procured separately by IRDA. The bidder will conduct the test based on the agreed test procedures as proposed by the bidder and agreed upon by IRDA, keeping in view IRDA‘s future load of transactional users. The solution shall not be cleared for Go-live (phase 2) unless the testing is conducted successfully and is cleared by IRDA.

4.27. Other Requirements:

4.27.1. **Open Source Software**: IRDA / IIB is looking for solution in the FAS space which is proven and has the functionality and features to meet the current requirements and grow into the future. The solution proposed should have been deployed earlier and meeting the requirements adequately. Robustness and Maturity of the application environment and the solution stack is extremely important and therefore, the bidders are refrained from using any open source product/software unless that open source product/software is accompanied by an Enterprise end user license agreement (EULA) that covers indemnification, warranty, maintenance and support.

4.27.2. **Audit Trails:** The solution should provide full audit trails for all the user activity. Logs shall be created to clearly indicate the fields where a change is made along with the credentials and time stamp. Additionally, logs shall be created for the system administrator to monitor any unauthorized access or attempt to access.

4.27.3. **Archival of old records:** All the data that enters the system shall reside permanently. However, the solution shall facilitate the archival of the old transactions/records beyond a specified period of time in the history. The archival methodology shall be a function of the analytics that will be generated and hence the bidder shall draw an archiving methodology clearly indicating the timelines, expectations and management of archived records. It may however be noted that authorized users shall be provided the ability to access the archived records for reference purposes. The bidder shall utilize an information classification program for data as per **International Standard ISO -15489,** which describes requirements to identify, retain, and protect records used in the course of business to ensure integrity with proper handling. The archived data shall be stored both in-disk as well as on an external media like tape in the custody of an authorized official of IRDA/IIB.

4.27.4. **Constraints:** It is mandatory that in case there are any technical and/or operational constraints as far as the components of the offered solution are concerned, these should be highlighted in the proposal. The constraints can be in terms of maximum number of users the system can handle at a given point of time, data handling limitations, integrating with other systems, or any other constraint of the proposed solution that the bidders is aware of.

Section 5:: Project Governance requirements

5.1. Preparation of the Project plan:

5.1.1. A detailed Project charter including the detailed Project Plan, indicating all activities with resources required with their roles and responsibilities and time schedule will be required to be prepared at the start of the project and submitted to IRDA/IIB for approval. It shall be the endeavor of the bidder to 'GO-LIVE' (including all phases) within a period not exceeding 18 months from the award of the contract. The project charter shall also contain brief project description, approach and methodology, milestones, project organization with their roles and responsibilities, project risks and mitigation plans, dependencies etc. Adequate framework should also be devised to measure the schedule variances, to identify dependencies and monitor the progress on a day-to-day basis. It is essential that the bidder walks the project plan with IRDA/IIB and obtains the sign off on the same.

5.1.2. IRDA/IIB and the selected bidder shall work together to develop a project plan and implementation strategy with periodic milestones and estimated timetable within a period of 45 days from the date of award of contract come up with the following at the minimum in furtherance of the objective of the project

- Finalisation of data policy after due data planning
- Data formats standardization.
- Identification of knowledge and third party databases for prediction and detection capabilities.
- Identification of master data, historical data from external sources.
- Identification of reporting requirements.
- Drawing health insurance processes for various analytics and setting up data ware house/data mart with optimal data loading schedules
- Finalization of any parameter or dependency with respect to any of the requirement, terms and conditions mentioned as a part of this RFP.

5.1.3. The bidder shall also include in the program plan for supplying, installing, hosting and implementing the software/hardware covered under this contract.

5.1.4. The bidder shall also propose a data policy as this Project is analytics intensive with heavy dependence on data, both internal and external and obtain approval from IRDA/IIB on outcomes of data planning, scenario building, results, improvisation, updates and related tasks.

5.1.5. The bidder is expected to identify all the dependencies and identify a redressal strategy and seek an approval with respect to the redressal being identified.

5.2. Project Site:

The proposed Project site is – IRDA/IIB Premises, Hyderabad and the bidder might have to travel to such a location as may be prescribed by the IRDA/IIB as a part of the project requirement. The cost of such travel and related expenses will be borne by the bidder himself.

5.3. Need for additional data and phasing of the project:

5.3.1. **Data Source:** The primary source of data for the project is the IIB, located at Hyderabad. It may be also be noted here that currently, there is no centralized repository of the past fraudsters/fraud data in the insurance sector. As such, the primary emphasis of the implementation agency shall be to utilize the transaction level data available with IIB. By utilizing the available data in the best possible manner, the IA shall endeavor to deliver "low hanging fruits" at an early date so as to ensure the acceptance and success of the project.

During the phase 1 of the project, the requirement for additional data (if any) needs to be clearly identified by the IA. In addition, the IA needs to propose for IRDA/IIB's consideration,

- Standardized data submission process
- Refinement in the existing data formats to meet the requirements of the FAS.

It is important here to note that the need for the additional data fields has to be substantiated by the analytics and the benefit thereby derived. Any requirement specified within the scope of work that has a specific dependency on additional data shall be addressed in phase 2 and subsequently on an on-going basis

5.3.2. **Analytics with available data**: Though the bidder is required to propose the requirements that are handled in phase 1 and 2, the following list indicates the requirements that may be grouped in each of these phases.

- Single repository for Fraud – Both
- Modeling with Anomaly detection capabilities – Both
- Scoring and Rule management – Both
- Triggers/Alerts: Both
- Regulating False-positives – Two
- Post Claims Analytics: One
- Summary tools: One
- Data quality: One
- Data standards: Two
- Data Structured -One
- Unstructured data analysis: Two
- Text mining: Two

- Data mining: One
- Reporting: One
- Profiling - Both
- Predictive capabilities - Two
- Link and Social network analytics - Two
- Knowledge database – Two

The bidder may validate the above by cross checking the available data of IIB and is required to confirm in their response concerning the feasibility of implementation of above functionalities in both phases.

5.4. Project deliverables:

5.4.1. **Scope of work**: The overall scope of work for the implementation agency as part of the FAS project shall include:

- **Requirements gathering and SRS preparation**: The bidder shall gather and document system requirements in a comprehensive manner for the services listed in the Requirement Specifications document. The bidder shall prepare a Software Requirements Specifications (SRS) document based on the functional requirements/technical requirements, its own assessment and in consultation with IRDA/IIB and its representatives. The bidder would need to obtain a final sign-off from IRDA/IIB on the requirements gathered and SRS before proceeding with the design and development of the FAS solution. It must be noted that
    - The requirements and specifications provided as part of this RFP are intended to describe salient aspects of the bidder‘s scope of work and provide sufficient understanding to the bidders for preparing proposals and should not be considered as exhaustive. The requirements will have to be detailed further as part of SRS preparation.

- **Design, development and testing of FAS application**: Bidder shall design, develop and test the FAS application for meeting the system requirement specifications finalized for the services. The solution design shall include the design of application architecture, information architecture, network architecture, security architecture etc based on the details provided in this document. On the basis of the application design signed off by IRDA/IIB or its representative, the individual applications shall be modeled and designed using relevant modeling and design languages like UML. The bidder shall use the signed off design for the development of the FAS application software. Bidder shall also be responsible for designing the testing strategy including preparation of test plan and test cases and conducting unit testing of various modules, integration testing, load testing, performance testing etc. The user acceptance testing of the FAS application shall be done by IRDA/IIB. The bidder shall provide all necessary support, including test scripts for user acceptance testing, setting up the required test environment, making seating arrangements and providing suitable computer systems & peripherals, to the agency for conducting acceptance testing. It must be noted that IRDA/IIB shall own the data and the IPR

for the FAS application and all its related components as per the Intellectual Property Rights Clause of the TCRFP.

- The bidder shall be responsible for providing hosting, required hardware and network components and related system software (operating system, patches, antivirus etc). The bidder will be also providing the services of installation, configuration and commissioning the hardware and network equipments. It should be noted that IRDA/IIB will not make any investment for hardware and network equipments and related platform/operating system/ system software etc. The bidder is required to offer services on his own and avoid sub-contracting for the above. This infrastructure has to be dedicated for the proposed solution of IRDA/IIB. IRDA/IIB will perform a Security Audit, by a 3rd party agency, of all components of FAS application and related hardware and networking infrastructure. The bidder is expected to provide all possible support for any agency/group appointed for the purpose of any type of testing/certification.

- **Traceability Matrix**: The bidder shall comprehend each requirement functional and technical requirement and has to break down the same to the extent possible. These broken down requirements shall be identified by unique identification. The bidder shall be responsible for building up and submission of a traceability matrix that identifies and tracks the same to the functional/technical (hardware and software) solution, user interface, external/internal system interfaces, testing, documentation and through every stage of the software development life cycle.

- **Documents to be provided**

The bidder shall be responsible for preparation of documents including User Manuals, Operations Manual, Administration Manual, Security Manual, Application Support Guide and others (if any) as per industry best practices and acceptable standards (e.g. IEEE/ISO specifications for documentation). The following is the indicative list of documents to be delivered by the bidder:

Deliverable	**Details**
Detailed project plan and inception report	• Pre-commissioning, operational and user Acceptance Testing Plan • Hardware design, delivery and installation plan • Network design, delivery and installation plan • Change management, Communication and • Training plan • Data migration plan • Warranty service plan • Risk management plan • Business Continuity Plan • Task, time, and resource schedules • Quality assurance and control process details • Technical and operational procedures which must include (but not limited to) detailing on methods, tools, techniques, SOP etc.

Software Requirement Specifications (SRS) document	The SRS document for the FAS application will cover the following aspects: • Software Functionality Requirements • Software Requirements Specifications and • Customization Requirements Specifications • Formats of all input (data entry) screens • Naming conventions followed for the tables and fields • Format of all reports that would be generated by the FAS application • Access control mechanisms, data security requirements and audit trails to ensure that databases are not tampered or modified by unauthorized users • External Interface Specifications
Software Design Document (SDD)	The SDD document for FAS application will cover the following aspects: • High level design and architectural views • User Interface design • Logical and physical component mapping • Collaboration & Sequence diagrams of components • Details of validation rules and constraints (Integrity / Check /Referential etc) to be applied • Business rules and processing logic used for all services • All database structure and detailed description of fields and tables • Data flow diagrams (DFD's) & entity relationship (ER) diagrams • Tools and techniques to be used
Detailed hardware and network design and specifications	This document will cover the following aspects: • Hardware sizing and specifications based on application requirements, traffic and load, usability, scalability and performance • Assistance in finding out suitable location for hosting the data center and disaster recovery sites
Unit and integration testing plan	This document will cover the following aspects: • Detailed test plans for comprehensive unit testing of various FAS application modules • Detailed test plans for comprehensive integration testing of FAS application
Unit and integration testing report	This document will detail unit and integration tests conducted and their results
Interface control document	This document will detail the interface characteristics of the external systems and interfaces and documents & agreements between interface owners. It will contain information on both the physical and data element requirements that are necessary to make the transfer of information between systems feasible
User acceptance testing plan	This document will detail test plans for user acceptance testing

Go Live Plan	The roll out plan will cover the following: • Roll out approach • Key dependencies • KPIs for successful roll out • Planned service disruption • Roll back strategy
Change management Strategy	This document will detail the change management, communication and training strategy in conformance with the need for change interventions, communication and training as analyzed and agreed with IRDA/IIB and PMU
Computer-based trainings (CBTs)	Computer based training modules for IRDA/IIB officials and the external stakeholders. Along with this, a comprehensive training plan needs to be developed
User manual for CBTs	This document will cover the following aspects: • Procedure for running the CBTs/deploying them on a Learning Management System (LMS) • Procedure for making changes (e.g. text changes) to the CBT
Implementation of various change management initiatives	Refer Change Management Specification Section
Communication package	This will be a set of different artifacts and tools for communication
Workshops/trainings completion report	This document will cover the following aspects: • Workshops/training conducted • Name/organization details of various participants in the workshops/trainings • Feedback formats • Procedure for making changes (e.g. text changes) to the CBT
Operational procedures Manual	This document will cover in detail the procedures for operating various modules of the FAS application
Administration procedures Manual	This document will cover in detail the procedure for administering various modules of the FAS application
Security Policy and Procedures manual	This document will detail out the security policy that will be applied to the FAS system and operations, will also detail out different procedures and formats required for operationalizing the policy
Strategic Control policy and procedures manual	This document will detail the policy for ensuring IRDA‘s strategic control over FAS project in general and FAS application and database in particular, will also detail the procedures required for operationalizing the policy

Go-live/ application launch Report	This document will cover the following aspects: • Release notes for the application delivery • Results of tests conducted on the FAS application immediately post go-live • Any issues/errors noted in the testing
Contingency plan document	This document will cover the following aspects: • Emergency response procedures • Data backup arrangements, procedures, and responsibilities • Data archiving strategy and procedures • Disaster recovery procedures and responsibilities • Business Continuity plan and procedures
Periodic progress reports	The periodic progress reports would summarize the following: • Results accomplished during the prior period • Cumulative deviations to date from schedule of progress milestones as specified in the agreed and finalized project plan • Corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule • Other issues and outstanding problems; proposed actions to be taken • Resources that the bidder expects to be provided by the IRDA/IIB and/or actions to be taken by the IRDA/IIB in the next reporting period
Exit Management Plan	The exit management plan should comprise of the following details: • A detailed program of the transfer process including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer; • Plans for the communication with such of the Implementation agency's staff, suppliers, customers and any related third party. • (if applicable) proposed arrangements for the segregation of the Implementation agency's networks from the networks employed by PROJECT and identification of specific security tasks necessary for an effective termination; Plans for provision of contingent support to IRDA/IIB and its Replacement Implementation agency for a reasonable period after transfer. This shall be governed by the switching over clause of the Terms and conditions of the RFP.
Source Code and IPR	The bidder should provide along with the source code, object code and systems specifications, the other library files used and third party propriety files used in running the software to IRDA/IIB without any cost and the IA shall provide the same along with other deliverables. If, IA updates / amends the codes, to complete the assigned contract in full, covered by the SRS pertaining to this Agreement or amended SRS to complete the assigned contract covered by this Agreement, and in doing so, if any third party propriety files, other library files are used, such files shall also be provided to IRDA on completion of the work, without any additional cost

	The source codes & intellectual property rights of all the software/ deliverable developed under this project shall be the exclusive property of IRDA. IRDA will have further rights to distribute the source codes based on its discretion. However, the Bidder shall submit a declaration to this effect.

5.4.2. **Project Timelines** The activities under scope of work (all phases) will need to be completed by the bidding party/bidder with in a period of eighteen months from the date of awarding of contract. It is the expectation of IRDA/IIB that the implementing bidding party/bidder will be in place within two weeks from the award of the contract. The tentative timelines shall be provided by the bidder as a part of the project plan.

5.4.3. **Data migration:** All the historical data needs to be entered to the current system. Data being migrated has to be rationalized, codified, transformed and reconciled to be suitably used for future purposes. All data upload/ download programs/ interfaces required to carry out the migration shall be carried out by the IA.

5.4.4. **Program Governance Steering Committee, Program Management Unit:** The bidding party/bidder will be responsible for minimizing project risk through periodic reviews of the implementation project. This will be at two levels, viz., steering committee for Management level Governance and Project management unit for both Technical review and Project management. The steering committee will have representatives from management teams of IRDA and the Vendor and also the Chairman of PMU will be a member of Steering committee. The purpose is to provide an objective review of the implementation of project including the solution approaches and to identify any risks to the project goals and recommend corrective action by conducting reviews in the following areas:

- Application, technical and project management
- IT infrastructure
- Organizational change management
- Sustained support and benefits achievement

5.4.5. **Solution, Technical and Development reviews**: This review helps to determine whether the design and implementation adheres to proven standards, such as upward compatibility where custom developments or enhancements to the systems are planned. The scope of this review is to study programs and applications that have been developed explicitly for IRDA/IIB. The feedback provided will mainly deal with ways and means of optimizing the custom developments to achieve better performance. The bidder shall perform a solution review covering the application design, business process parameters, software, hardware and databases. To review the business model proposed and configured in the system. In addition, a technical review of components and operational procedures, such as security, backup, performance management, printing, desktop operations etc.,

shall also be performed. The project plan should include details with regard to the periodicity and process to be followed for the reviews.

5.4.6. **Go Live**: The Bidder is required to demonstrate to the satisfaction of IRDA/IIB the following:

- A dashboard containing the functionalities from 3.1 to 3.11 stated above
- Successful data exchange between Insurers, other stakeholders and the solution
- Successful completion of the UAT, security audit, performance and load testing and DR drill.
- Other conditions as prescribed in Parts 1 and 2.

5.4.7. **Final Acceptance:** The final acceptance would be based on adherence to required response time, the integrity of the software after installation with no operational bugs. This would include fine tuning of the software, ensuring all required related component software are installed and no debugging is required. The acceptance tests should be carried out within a month of Go-live for each major module and after a report is submitted on the successful conclusion of these tests. The commissioning/ implementation of the software shall be deemed complete only after the satisfactory acceptance by the IRDA/IIB management. The evaluation methodology and results have to be validated with IRDA/IIB and a report should be submitted for review and approval by IRDA/IIB's management.

5.4.8. **Approval/Signoff:** Every deliverable shall undergo an approval/signoff process.

5.4.9. **Continuous Improvement to deliver an effective system:** The solution shall provide scope for a continuous improvement to the fraud prediction and detection framework to incorporate the following at the minimum

- The newer techniques that emerge on a regular basis in the insurance domain
- Experiences of the domestic insurers from the use of the Fraud Analytics system that is being implemented as a part of this project.
- New learnings from the day to day predictive and detection analysis done as a part of this system
- Changes as may be relevant with the changing times, challenges, market dynamics or regulatory requirements.
- Newer technologies, upgrades to any off the shelf product/plug-ins that widens the scope of the fraud analytics.
- Checks to ensure that the false positives are maintained at a bare minimum.

The bidder shall indicate the possible strike rate (ratio of cases concluded as fraud by the users to cases identified by the system as fraudulent) of the fraudulent alerts against the parameters defined. The strike rate indicates effectiveness of the system and the bidder shall at all times strive to achieve the strike rate indicated to IRDA/IIB on an ongoing basis. A monthly report of strike rate, alerts closed without action vis-à-vis the alerts generated shall be submitted to IRDA/IIB to assess the effectiveness of the system. Adequate emphasis shall be given to identify and ensure that the

false negatives are minimized as well. To achieve the purpose stated above, auto profile calibration and periodic model recalibration shall be essential. The changes made as a part of continuous improvement exercise will be governed by the Annual Maintenance Service and Change Management clauses stated within this RFP.

Section 6: Miscellaneous

6.1. Installation, Maintenance and Monitoring:

6.1.1. **Systems Installation**: Supply, Installation, Administration and Management of Systems software, hardware, data, applications, network, security and related matters shall be the responsibility of the bidder. No existing license can be leveraged as such; all the licenses shall be procured for the use of FAS.

6.1.2. **Inspection and Tests:** Following broad test procedure will generally be followed for inspection and testing of the Systems that are commissioned for this project (at the project site or any alternate site). –

- The Bidder will dispatch the systems to the Project site after internal inspection testing along with the Bidder's inspection report and manufacturer's warranty certificate. The IRDA will test the equipment after completion of the installation and commissioning at the project site. Complete hardware and software as specified in the Bidders proposal should be supplied, installed and commissioned properly by the Bidder prior to commencement of performance tests.
    - Acceptance of the system will be based on the following criteria and to the IRDA/IIB's satisfaction:
    - Successful test of all required and proposed functions with no defects.
    - Successful demonstration that the system performance is as required and proposed
    - Successful completion of all required training; and Delivery of the complete documentation set to the IRDA.
    - Successful conduct of security audit and Disaster recovery drill (Costs related to these shall be borne by the bidder).
    - The users and support organization are adequately trained
    - The system contains a correct and complete set of data
    - The system complies with functional requirements specifications controllable and agreed post go live support agreement is in place
    - System authorizations for both users and support-organization are in place

- The acceptance-testing with respect to the installation of these systems is for a period that must be mutually agreed upon with the bidder, but cover no less than thirty (30) trouble free days. Should hardware or software failures occur during this period, the Bidder must take any

necessary actions to correct the failure, and then the thirty (30) day trouble free period gets restarted. More than three failures of the same type may be deemed a total failure, and may terminate the acceptance test and cancel the recommendation for purchase. The acceptance test period will be part of the implementation plan. The Bidder must agree that failure on the part of the Bidder to correct a functional or technical deficiency in the Bidder's specified solution shall be deemed to be a total failure, and the IRDA, at its option, may terminate the acceptance test and cancel the recommendation for purchase.

- The acceptance test will be conducted by the IRDA/IIB, with the help of their consultant or any other person nominated by the IRDA/IIB, at its option and in the presence of the bidder. The successful conclusion of the acceptance test for the installed systems and equipment shall be the sole responsibility. There shall not be any additional charges for carrying out acceptance tests.

- The inspections and tests may be conducted at the premises of the Bidder and/or at the Project site. If conducted at the premises of the Bidder, all reasonable facilities and assistance shall be furnished to the IRDA/IIB's authorized representatives at no charge to the IRDA. Bidder shall intimate to the IRDA/IIB indicating that the system is ready for inspection and the IRDA can send their authorized representatives for inspection at project premises. After receipt of such intimation from the Bidder, the IRDA/IIB shall arrange for pre-dispatch inspection and test. After the computer system passes in the inspection and tests, the Bidder shall deliver and install the system at the Project site.

- Should any inspected or tested systems fail to conform to the specifications, the IRDA may reject the systems and the Bidder shall either replace the rejected systems or make alterations necessary to meet specification requirements free of cost to the IRDA/IIB.

- The Purchaser's rights to inspect, test and, where necessary, reject the systems after the systems ' arrival at Project Site shall in no way be limited or waived by reason of the systems having previously been inspected, tested and passed by the IRDA/IIB or its officials prior to the systems shipment.

6.1.3. System performance auditing and monitoring

The bidder shall be responsible for monitoring and tracking of the solution to ensure proper functioning without any unprecedented failures. It is expected that on a periodic basis, a review is done of the quantum of utilization, processing efficiency, memory and storage utilization and all such related aspects. A report on this shall be placed with the PMU invariably.

6.1.4. System collaboration

The system should be able to collaborate with the databases of external IT systems with Insurers, Intermediaries and third party databases in addition to IIB database. The data from these external systems will be used for reporting and analytics. The system should also be able to integrate with standard day to day applications like MS Office (MS Word, MS Excel) and MS Outlook. For identity management, the bidder should ensure the integration of the system to the existing authentication provider (MS Active Directory) to ensure single sign on.

6.1.5. External integration

The implementer shall ensure the data retrieval and entry in external IT systems for, but not be limited to the following:

- Inter operability with any standard mailing software for unified mailing and messaging including relay service
- Inter operability with IIB database for data integration
- Inter operability with Third party databases for data integration

The scope of external integration will be to:

- Ensure that only the required data is transferred to FAS solution from the external systems
- Ensure that all interfaces are self checking so that any exceptions or data validation errors are reported by the system

Ensure integration logs are maintained to confirm the success or otherwise of the interface, complete with control totals

6.1.6. Operation and Maintenance Requirements

The bidder shall provide Operations and Maintenance (O&M) support for 5 years from the date of FAS application go-live (phase 2). The following sections detail the O&M requirements.

- **Application Management**

  - The bidder shall be responsible for defect free operation of the FAS application during the O&M period and ensuring its 24x7 availability at all the end-user locations and across all the channels of access. Any bugs reported in the application shall need to be fixed within a time frame mutually agreeable to both IRDA/IIB and the bidder.
  - The bidder shall also be responsible for version control of the application files and shall need to update application documentation to reflect the current features and functionality of the application.
  - The bidder shall provide a staging environment in the data center for testing of changes/ patches before applying them on production environment.

- **Infrastructure Management**
  - Infrastructure management includes overall management and administration of entire IT and non-IT infrastructure including servers (including server operating system), network components, storage devices, UPS, DG sets, air-conditioners, etc. The bidder, on its own shall be responsible for the following activities as part of infrastructure management:
- **Incident management**
  - Provide resolution to incidents as per the resolution time limit agreed upon with IRDA/IIB
- **Problem management**
  - Perform root cause analysis for infrastructure problems/recurring incidents and initiate request for change
  - Schedule and complete preventive maintenance activities
- **Business continuity management**
  - Provide necessary support in ensuring business continuity at end-user locations configuration management
  - Maintain asset register for all server and ancillary (like UPS, printers etc.) equipments. Record information such as serial number, asset code, warranty and AMC details. Exact details to be recorded will be finalized in consultation with IRDA/IIB.
  - Maintain a database of server count and configurations
- **Availability management**
  - Review key monitoring parameters (to be finalized in consultation with IRDA/IIB) from availability point of view
  - Performance tuning of the system to enhance system‘s performance and comply to SLAs on a continuous basis
  - Provide prior communication on outages as per agreed communication processes
  - Ensure availability of sufficient critical spares, sufficient consumable spares at all relevant locations
  - Ensure availability of consumable spares.
- **Monitoring management**
  - Preparation of monthly dashboard on monitoring coverage, alerts generated/ closed, alerts escalated and other hits/ misses

- **Backup management**
    - The bidder should evolve a backup and archival strategy
    - Regular backups of project related data
    - Media management like inter and intra city tape transfers
    - Handling service requests on backup and restoration
    - Generation of monthly report on the backup/restoration performance
- **Security management**
    - 100% antivirus coverage with patterns not more than one week old on any given system
    - Reporting and resolution of security incidents
    - Maintaining secure domain policies
    - Vendor management
    - Escalation and co-ordination with other vendors for problem resolution
- **Disaster recovery management**
    - Managing Disaster Recovery activities pertaining to data center operations
- **General administration and support**
    - Providing suitable access to PMU, designated by IRDA/IIB, to tools implemented for monitoring infrastructure components
    - Creation/deletion/modification of user accounts at the OS level
    - Periodic review of user privileges at the OS level
    - Password management
    - Any other day-to-day administration and support activities required
    - Clean up / archival of FAS system logs operation
- **Network management**
    - The bidder shall be responsible for management and administration of the wide area network. The broad activities would include:
    - Incident management
    - Provide resolution to incidents as per the resolution time limit agreed upon with IRDA/IIB
- **Problem management**
    - Root cause analysis for infrastructure problems/recurring problems and initiate request for change
    - Scheduling of maintenance activities

- **Change and release management**
    - Maintain records of all hardware and software installation (new networks and network devices, initial routes, Policy configuration), movement, addition and change (IMAC) in a configuration database
    - Perform impact analysis, create test plan, rollback plans
    - Post implementation review and documented closure for all changes and tracking all changes implemented
- **Availability management**
    - Review of key monitoring parameters from availability point of view
    - Provide communication on outages as per agreed communication processes
    - Ensure availability of critical network spares
- **Monitoring management**
    - Monitoring critical parameters of all network elements (CPU and memory utilization), links availability and utilization, latency and reporting
- **Backup management**
    - Backup of all network device configurations
    - Media management like inter and intra city tape transfers
    - Handling service requests on backup and restoration
    - Generation of monthly report on the backup/restoration performance
- **Security management**
    - Daily Review of logs daily that are of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability, Security alerts and responses. Proactive measures in the event a problem is detected.
    - Policy management (firewall users, rules, hosts, access controls, daily adaptations)
    - Modify security policy, routing table and protocols
    - Troubleshooting firewall/anti-spamming/web security hardware related issues and coordinating the replacement of hardware
- **Vendor management**
    - Escalation and co-ordination with other vendors for any problem resolution

- **General administration and support**

    - Providing suitable access to PMU, designated by IRDA/IIB, to tools implemented for monitoring infrastructure components
    - Disabling/enabling services/ports
    - Any other day-to-day administration and support activities required

6.1.7. **Change Management:**

For the software/hardware upgrade: IRDA/IIB expects the bidder to create and maintain effective communication and facilitate change thereby ensuring the successful adoption of the new system. The bidder will provide communication strategy and relevant material to support communication as part of change management initiative. The bidder needs to understand the functional and technical requirements before the SRS sign-off and design the application appropriately. Changes to the requirements thereafter will need to undergo Change Request Approval process with cost estimate as per Annexure 8 and as agreed at the time of award. Please refer to the clause on AMS also.

For software/hardware maintenance:

- Ensure that any component change due to any fault is replaced with a component of the same make and configuration
- Maintain records of all hardware, software installation, movement, upgrade, addition and change (IMAC) in the configuration database.
- Perform impact analysis, create test plan, and develop rollback plans

6.1.8. **Business continuity management**

Provide necessary support to IRDA in ensuring business continuity at end-user locations

6.1.9. **Helpdesk support**

The bidder shall set up an appropriately staffed and centralized helpdesk for providing helpdesk support to various users of the FAS application. The helpdesk team should comprise of adequate team members for support on a continuous basis in the onsite support phase. The broad set of activities as part of helpdesk support includes:

- Receiving incidents/requests through phone, email and other means. Entering of the incidents in the helpdesk application and informing the user of the unique incident id generated through email
- Routing incidents internally between teams and tracking till resolution
- Providing updates to users on incidents logged
    - Periodic reporting of incidents providing details including (but not limited to) number of incidents reported, reporting mechanism (phone/ email)

- Escalation of any untoward incidents to IRDA/IIB on an immediate basis either for reporting purposes / action from IRDA/IIB.

6.1.10. **Implementation of SLA monitoring system**

The bidder shall design and implement an SLA measurement & reporting system to measure and report performance of the solution against the service levels specified in ***section on Service Level Agreement***. The system shall also allow calculation of quarterly payments to the bidder and any rewards and penalties as specified by IRDA/IIB.

The SLA measurement & reporting system shall be reviewed and certified by a third party audit agency before project go-live and start of operations. IRDA/IIB officials and MU personnel shall be provided real-time access to the system. Additionally, IRDA/IIB designated personnel should be provided administrative privileges to the system as per the agreed role assigned for them.

6.1.11. **Data and information security requirements**

Given the need to maintain confidentiality of data about insurers and intermediaries, a strong and comprehensive information security policy based on leading standards such as ISO 27001 and guidelines from Department of Information Technology (DIT) would need to be defined and implemented by the bidder. The same should be approved by IRDA/IIB and must be adhered by IA at all times during the currency of the contract.
At the minimum the policy should define the following guidelines:

6.1.12. **Inventory of assets**

An inventory of all hardware and software assets should be maintained and updated periodically

6.1.13. **Information classification**

Information within the system should be classified as:

- Public
- Confidential
- Restricted

Access to the information should be provided based on the classification of the information. Data owners should nominate appropriate information classification on their data and should review information classification periodically to determine if current classification levels are valid.

6.1.14. **Human resource security**

Background check should be performed on all individuals for whom access to the FAS system is requested. Access should be revoked when a user leaves the organization or does not require access to the application. User accounts of any outsourced agency personnel should include an automatic account expiration date, set at no longer than 6 months from their start date or till expiry of contract whichever is earlier.

Any personnel of the bidder who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has information security implications, will immediately report the incident to the designated IT in-charge. Any personnel found violating the IS policy would be penalized.

6.1.15. **Communications and operations management**

All operations performed by third parties should be monitored periodically.

6.2. Testing:

6.2.1. **Unit/Integration testing:** The bidder shall prepare procedures detailing the steps for conducting unit and integration tests and shall conduct tests to demonstrate that the system meets all the requirements (functional and technical) in the specifications as brought out in this request for proposal and would be in accordance with the procedures detailed in approved SRS document before it is deployed for User Acceptance Testing. These tests shall be conducted to the satisfaction of all the stakeholders that IRDA/IIB identifies.

6.2.2. **User acceptance testing:** The bidder shall develop the acceptance test procedures in mutual agreement with IRDA/IIB and shall facilitate conducting these tests to demonstrate the conformance to the required process maps and operations response times. IRDA/IIB shall form a UAT team for conducting these tests. The acceptance tests should be carried out before the Go-live and a report is to be submitted on the successful conclusion of these tests. Any function will be allowed to Go-live only after the successful conclusion of the UAT tests. These tests shall be conducted to the satisfaction of all the stakeholders that IRDA/IIB identifies. In an eventuality where the IRDA/IIB 's testing team opines that the overall quality of the development/coding is inferior, roll back of the code to the development environment shall be done. IRDA/IIB shall share the list of all identified defects duly categorized. It shall be the responsibility of the bidder to rectify all the issues before delivering the code for re-testing.

6.2.3. **Load and stress testing:** Loading, scalability and stress tes□ng would be conducted prior to —Go-Live, once the system testing and integration testing of the configured and customized solution has been conducted successfully. The strategy as well as draft procedure for stress and load testing in view of future load of users shall be proposed by the bidder and approved by IRDA/IIB. Based on the recommendations, the testing tool will be procured separately by IRDA/IIB. The bidder will conduct the test based on the mutually agreed test procedures as proposed by the bidder, keeping in view IRDA/IIB's future load of transactional users. The solution shall not be cleared for Go-live unless the testing is conducted successfully and is cleared by IRDA/IIB. Also, the bidder shall prepare a bench mark suite and demonstrate the capabilities of the system to adhere to these bench marks on a half-yearly basis from the date of 'Go-Live' to ensure that the different types of loads are handled

appropriately and also to ensure that the sizing of the systems is appropriate from time to time. To achieve this purpose, reports shall be submitted to IRDA/IIB.

6.3. Training, Capacity building, Warranty and Support.

6.3.1. **Capacity building**: The solution provider shall provide necessary training to the resources identified by IRDA on using the system, altering and updating the models developed, application, database, network, hardware monitoring and maintenance etc. The primary focus shall be on using the system for non-IRDA/IIB resources. For IRDA/IIB resources, focus shall be on using/updating the models and administering the system (application, network, database, etc.,) as well. It may be assumed that there would be around 150 people to be trained in a class room session at Mumbai, and 100 at Hyderabad. These sessions shall be on multiple dates (at least 4 in number at each of the locations). A detailed training calendar should be prepared based on the training needs identified. The cost of travel for bidders own staff, infrastructure and other arrangement for these sessions shall be borne by the bidder. Additionally, to address any integration related issues and issues that need a technical support for the external interfacing, two sessions shall be planned (one at Hyderabad and one at Mumbai) at the cost of the bidder to facilitate the external entities in integrating with the proposed system. The bidder shall provide necessary class room and instructor led training/hand holding to the users. In addition, the solution shall include creation of online help files/tutorials/video demonstrations/faq's section/'how to' section/new user orientation guide and a process to raise queries to the system administrator and obtain requisite feedback. The user manuals for the various modules within the system shall also be devised. All the content stated above shall also be available for authorized online access. Quick reference guides and release notes as a part of the change management shall also be devised. The quality of the training provided shall be assessed by IRDA/IIB against a set of metrics in consultation with the bidder. The bidder may have to repeat all or parts of the training based on the quality assessment carried out by IRDA/IIB.

6.3.2. **Training tools**

The bidder shall arrange required training tools for providing various essential trainings. Adequate training material which includes training manuals, quick reference cards etc. should be provided during the training sessions. The recommended training material can be in paper / electronic media, business process overview, job activity training, and delivery options being online, instructor led class rooms, etc.

6.3.3. **Post go-live stabilization**

The bidder shall provide post 'GO-LIVE' support as a part of this project, by deputing technical consultants at IRDA/IIB for a period until six months from the date of phase 2 'GO-LIVE', at no additional cost. The consultants with required competency shall provide quick solution to all related

issues/ complaints. During the stabilization period, the bidder shall help IRDA/IIB users to troubleshoot transactions and reports, build/update user manuals and configuration manuals. In addition, post 'GO-LIVE' stabilization shall address issues/bugs/discrepancies pertaining to the delivered functionality that was assured/assumed to be working at the time of 'GO-LIVE'.

6.3.4. **Annual maintenance support (AMS):** The bidder shall provide, support and maintenance of the entire solution designed, developed, implemented and operationalized as part of this project for the entire contract period (from the date of phase 2 GO-LIVE). This shall include maintenance of the application and all other standard third party software wherever applicable as a solution for the contract period. The periodicity of the AMS charges payment shall be quarterly.

- The AMS shall be provided by trained and experienced personnel of the bidding parties. The service level for IRDA/IIB's problem resolution shall be defined by the response time and time taken for successful resolution.

- Apart from the above, the bidder will also be required to generate ad-hoc/on-demand report/query, data on system configuration, upgrades and performance in general, as and when required by IRDA/IIB within a period of 24 hours from the time of receipt of the request from IRDA or released by an OEM.

- The requests under the AMS clause shall fully comply with the SLA's stipulated for the same. Non-adherence of these service levels shall amount to a breach of contract, which may initiate the appropriate liquidating damage.

Any change in report /formats /user interface which requires an estimated effort of not more than 10 man days during the maintenance period, shall be executed by the bidder without any charge to IRDA/IIB. Effort estimation more than 10 man-days during the maintenance, shall attract the change management cost and IRDA/IIB shall pay to bidder for the change order as per the charges accepted for change management.

6.3.5. IRDA/IIB expects the bidder to create and maintain effective communication and facilitate change thereby ensuring the successful adoption of the new system. The bidder will provide communication strategy and relevant material to support communication as part of change management initiative. The bidder needs to understand the functional and technical requirements before the SRS sign-off and design the application appropriately. Changes to the requirements thereafter will need to undergo Change Request Approval process with cost estimate as per Annexure 8. Please refer to the clause on AMS also.

- Sustained support and benefits achievement
- Schedule compliance

There would be at least one such cycle each quarter during the project implementation depending on the need, deliverables and project timelines.

Section 7:: Service Level requirements:

The bidder shall at all times ensure adherence to the Service Level Agreements (SLA's) as stipulated in this document. In striving towards achieving the SLA's, the bidder shall comply with the following:

7.1. The bidder shall provide an Availability Report on monthly basis and a monthly report shall be provided to the authority at the end of every month containing the summary of all incidents reported and associated bidder performance measurement for that period for a review. The bidder shall be responsible for the performance of the SLA's of the vendors/manufacturers of the products forming part of the solution.

7.2. Performance measurements would be assessed through audits or reports, as appropriate to be provided by the bidder e.g. utilization reports, response time measurements reports, etc. The tools to perform the audit will need to be provided by the bidder. Audits will normally be done on regular basis or as required by IRDA/IIB and will be performed by the IRDA/IIB or IRDA/IIB's appointed third party agencies.

7.3. Critical and Key infrastructure of Data Center and Disaster Recovery Site will be supported on 24x7 basis.

7.4. Downtime shall commence when either the DC or the DR fails.

7.5. Uptime will be computed based on availability of the applications to IRDA/IIB's users irrespective of availability of servers either individual servers/clusters. Also, non compliance with performance parameters for business, network and environmental infrastructure and system / service degradation will be considered for downtime calculation.

7.6. A breach will occur when; the bidder/consortium partner fails to meet Minimum Service Levels, as measured on a periodic basis, for a stated Service Level.

7.7. In the event of a breach, the bidder shall pay the authority a penalty that will be computed in accordance with the following formula:

7.8. Breach = ABS (Actual Service Level (only when below the lower service level) – Desired Minimum Service Level)

7.9. Penalty = Breach X (Equated Total Implementation Fees Charged by the bidder)

7.10. In the event that a breach has occurred for more than one service level requirement, the sum of the corresponding penalties shall be imposed.

7.11. The SLA measurement tool designed & developed by bidder shall be tested and certified for its accuracy, reliability and completeness if required by a 3rd Party agency before it is deployed.

7.12. If the SLA measurement tool and/or data equivalent to more than 5% of sample size is missing or unavailable for a particular SLA metric or if the tool is found to be unreliable then the quarterly credit for that metric would be counted as Zero (or lower if specified).

7.13. If service level for any of the critical metrics (availability) is lower than the expected in three months consecutively then IRDA shall have the right to invoke penalty of 3% of total quarterly amount payable to bidder. For any other metric this penalty will be 1% instead of 3%. Penalty shall be adjusted to the final quarterly amount payable to bidder based on the level of conformance to the service level expected.

7.14. In case of one breach in the SLA, IRDA/IIB shall have the right to invoke penalty of 10% of total quarterly amount payable to bidder. In case of two or more breaches in a quarter or breach of a

particular SLA metric consecutively in two quarters, IRDA/IIB shall have the right to invoke full PBG and/ or call for termination of contract. Penalty shall be adjusted to the final quarterly amount payable to bidder based on the level of conformance to the service level expected.

7.15. If the overall penalty applicable in any quarter during the currency of the contract exceeds 20%; then IRDA/IIB shall have the right to terminate the contract.

7.16. The total amount of penalty that the bidder is obligated to pay to IRDA/IIB shall be reflected on the invoice provided in the quarter after the quarter in which the Service Levels were assessed. IRDA shall be entitled to deduct the penalty amount from the amounts payable by IRDA/IIB to the bidder as per the invoice.

7.17. For the purposes of the SLA's,

7.17.1. "Scheduled operation time" means the scheduled operating hours of the System for the month. All planned downtime on the system would be deducted from the total operation time for the month to give the scheduled operation time.

7.17.2. "System downtime" subject to the SLA, means accumulated time during which the System is not available to the IRDA/IIB's users due to in-scope system or infrastructure failure, and measured from the time IRDA/IIB and/or the external stakeholders log a call with the bidder's help desk of the failure or the failure is known to the bidder from the availability measurement tools to the time when the System is returned to proper operation.

7.17.3. SLA's monitoring: The SLA parameters shall be measured on a periodic basis as per the individual SLA parameter requirements, through SLA Measurement tools to be designed by the bidder for the purpose and audited by a 3rd party audit agency for accuracy, reliability and completeness. If the performance of the system/ services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of IRDA/IIB or an agency designated by IRDA, then IRDA will have the right to take appropriate corrective actions including termination of the contract. The SLA shall be reviewed on an annual basis as IRDA/IIB decides after taking the advice of the bidder, PMU (Project Management Unit) and other agencies. All the changes to be made would be decided by IRDA/IIB after consultation with the bidder. The changes made should not result in undue financial advantage to the bidder.

7.17.4. The bidder will get 100% of EQI (Equated Quarterly Installments) if the Expected Service levels are fully achieved in the assessment of IRDA /IIB/ PMU (Project Management Unit). The Operation and Maintenance SLA will commence from the date when the Project Implementation has been completed to the satisfaction of IRDA/IIB, certified in accordance with the terms of this Agreement and the system has been declared "Go-Live" by IRDA/IIB and shall run for a period of five years from the date of phase 2 "Go-Live".

7.18. **SERVICE LEVEL AGREEMENT (SLA's)**

The following table presents the SLAs for this project. The bidder shall at all times ensure that the SLA's are met and ensure that for any part of the SLA having a dependency on a third party, the bidder alone shall take the responsibility to comply. IRDA reserves the right to negotiate the service level agreement with the bidder at the end of every year post Go-Live.

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
	Availability Parameters					
1	Overall availability of web services Including statefulness, authorized access	>99.5 %	-	<99.5%	Monthly	• Analysis of event log performed through use of automated tools • Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA appointed agency for review/report through automated tools. • During these periods all web services should be available and there should be no performance degradation including web services time-outs at that time.
2	Time window Availability for batch operations, wherever applicable	<4 hours (excluding back-up time)	> 4 hours - <=6 Hours (excluding back- up time)	>4 hours (excluding back-up time)	Monthly	• Analysis of event log performed through use of automated tools • Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA/IIB/their appointed agency for review/report through automated tools.

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
						• End-to-end loop back mechanism must be established for checking the availability of services back-up time. • In case the time window for batch operations is exceeded the additional time will be considered for system downtime calculation.
3	System Response Time	End to end response time should be < 2 seconds (end user to core application and back)	End to end response time should be > 2seconds-<= 6 seconds (end user to core application and back)	End to end response time > 6 seconds (end user to core application and back)	Monthly	• Analysis of event log performed through use of automated tools Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA appointed agency for review/report through automated tools • End-to-end loop back mechanism must be established for checking the availability of services
4	System support for concurrent users	Support 1120 concurrent users	Support >1000 but < 1120 concurrent users for internet portal	Support <1000 concurrent users for internet portal	Monthly	• Analysis of event log performed through use of automated tools • Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA appointed agency for review/ report through automated tools • End-to-end loop back mechanism must

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
						be established for checking the availability of services
5	Disaster Recovery Site Availability	Business Operations to resume	Business operations <=75 minutes of the Data Centre failing.	Business operations to resume from Disaster Recovery Site > 75 minutes of the Data Centre failing.	Monthly	• Analysis of event log performed through use of automated tools Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA Appointed agency for review/report through automated tools • End-to-end loop back mechanism must be established for checking the availability of services
6	Backup Success Rate	>99.5%	>99.5%-<=98.5%	<98.5%	Monthly	• Analysis of event log performed through use of automated tools Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA appointed agency for review/report through automated tools • End-to-end loop back mechanism must be established for checking the availability of services
7	Application Down time	Each planned down - time for application,	Each planned down - time for application,	Each planned down - time for	Daily	• Analysis of event log performed through use of automated tools • Bidder shall ensure that all relevant events are logged and such logs are

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
		database and operating system be< 4 hours.	database and operating system will be >4-<=6 hours.	application, database and operating system will be more than 6 hours.		made accessible to IRDA appointed agency for review/ report through automated tools • Each planned down – time for application, database and operating system will not be carried out during business hours. However, such activities which require more than 4 hours or required to be carried out during business hours will be scheduled in consultation with the Authority. In case the downtime exceeds the planned hours the additional time taken for servicing will be considered for infrastructure or system downtime as per availability measurements table.
8	Software Service Requests	>99.5%	>99.5%-<=98.5%	<98.5%	Daily	• Automated tool will be adopted for measurement of the resolution time • Bidder shall maintain relevant records and logs for this purpose
9	IT Policies & Procedures Management	>99.5%	>98.5%-<=99.5%	<98.5%	Fortnightly	• Automated tool will be adopted for measurement of the resolution time • Bidder shall maintain relevant records and logs for this purpose
10	Incident	>99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
	Management					records and logs for this purpose
11	Availability of all services over Internet/ Intranet/ VPN	>99.7%	>99.0% <=99.7%	<99.0%	Monthly	• Analysis of event logs performed through use of automated tools • Bidder shall ensure that all relevant events are logged and such logs are made accessible to IRDA appointed agency for review/report through automated tools • End-to-end loop back mechanism must be established for checking the availability of services • Non- availability of even one of the agreed services would amount to no service available for the purpose of this SLA and thus breach.
	Performance Parameters					
12	Average turnaround and page loading (this includes home page and graphical interfaces, visualization) time for transactions	<=2 seconds	>2 seconds – <=3 seconds	>3 seconds	Daily	• Automated tool will be adopted for measurement of this time. It will be tested using 4test transactions per hour (2 on Internet/ VPN and 2 on Intranet) • Measured over a leased circuit or equivalent of 256 Kbps • Measured as the elapsed time

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
						between the action link/button being clicked and its response page appearing completely • Test data to be identified distinctly and path taken by test data to be similar to real transaction • DNS servers should simulate access by end user and not answered locally • Cache to be cleared before every transaction used for measurement • Average must be achieved with more than 90% of the transactions being within 2 seconds and 9% of the transactions being within 2-3 seconds range
13	Average Document upload time for transactions on application	<=40 seconds	>40 seconds – <=60 seconds	> 60 seconds	Daily	• Automated tool willbe adopted for measurement of this time. It will be tested using 2 test transactions per hour (1 on Internet/ VPN and 1 on Intranet). • Measured over a leased circuit or equivalent of 256 Kbps with a test document payload of 1 MB. Measured as the elapsed time

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
						between the action link/button being clicked and its response page appearing completely • Test data to be identified distinctly and path taken by test data to be similar to real transaction • DNS servers should simulate access by end user and not answered locally • Cache to be cleared before every transaction used for measurement • Average must be achieved with more than 90% of the transactions being within 40 seconds and 9% of the transactions being within 40-60 seconds range
14	Resolution of end-user related incidents reported at the helpdesk	<=30 minutes	>30 minutes - <=1 hour	>1 hour	Daily	• Automated tool will be adopted for measurement of the resolution time • Bidder shall maintain relevant records and logs for this purpose
Helpdesk and Application Support (As mentioned in Helpdesk Support section in volume I)						
15	Average Speed of Answering calls	Average Speed of	Average Speed of Answering	Average Speed of Answering	Daily	• Bidder shall maintain relevant records and logs for this purpose

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
		Answering calls < 90 seconds for help desk	calls >90-<=120 seconds for help desk	calls >120 seconds for help desk		
16	Call abandon Rate	Call abandon rate should not exceed 6% for calls > 45 seconds	Call abandon rate should not exceed 6%-8% for calls > 45 seconds	Call abandon rate exceeds 8% for calls > 45 seconds	Daily	• Bidder shall maintain relevant records and logs for this purpose
17	Helpdesk Resolution time	cycle time =24 hours	cycle time >24-<=36 hours	Cycle time Of >36 hours	Daily	• Bidder shall maintain relevant records and logs for this purpose
18	Annual Maintenance Support (AMS) turnaround time – for tasks other than change requests. This includes adhoc/on-demand reports required by IRDA/IIB.	cycle time =24 hours	cycle time >24-<=36 hours	Cycle time Of >36 hours	Daily	• Bidder shall maintain relevant records and logs for this purpose

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
19	Routing of non Vendor supported actions	>=99.5% cases	>99.5%-<=98.5% cases	<98.5% cases	Monthly	• Bidder shall maintain relevant records and logs for this purpose
20	Notification to Users	>=99.5% cases	>99.5%-<=98.5% cases	<98.5% cases	Monthly	• Bidder shall maintain relevant records and logs for this purpose
21	Notification to Users	>=99.5% cases	>99.5%-<=98.5% cases	<98.5% cases	Monthly	• Notifying users in advance for all known (planned maintenance) problems • Bidder shall maintain relevant records and logs for this purpose
22	Provide reports	>=99.5% cases	>99.5%-<=98.5% cases	<98.5% cases	Daily	• Provide SLA compliance reports, monitoring and maintenance related MIS reports
23	Critical calls resolution time	Critical calls to be resolved within 2 hours from call received/logged whichever is earlier	Critical calls to be resolved within 2-4 hours from call received /logged whichever is earlier	Critical calls Are not resolved within 4 hours from call received / logged whichever is earlier	Daily	• Bidder shall maintain relevant records and logs for this purpose
24	Major calls resolution time	Major calls to be resolved within 6	Major calls to be resolved within 6-8 hours from	Major calls are not resolved within 8	Daily	• Bidder shall maintain relevant records and logs for this purpose

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
		hours from call received/logged whichever is earlier	call received /logged whichever is earlier	hours from call received/logged whichever is earlier		
25	Minor calls resolution time	Minor calls to be resolved within 24 hours from call received/logged whichever is earlier	Minor calls to be resolved within 24-36hours from call received /logged whichever is earlier	Minor calls Are not resolved within 36 hours from call received/logged whichever is earlier	Daily	• Bidder shall maintain relevant records and logs for this purpose
	Training					
26	End User Training for Applications	100% of users of IRDA shall be Appropriately trained prior to any implementation	80%-100% of Users of IRDA shall be Appropriately trained prior to any implementation	80% of Users of IRDA are not Appropriatel y trained prior to any implementation	Monthly	• Bidder shall maintain relevant training attendance records for this purpose
27	System Administration	>=99.5% of Admin	>98.5%-=99.5%	<98.5% of admin	Monthly	• Bidder shall maintain relevant training attendance records for

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
	for Applications Training	users shall be Appropriately trained prior to any implementation	of admin users shall be Appropriately trained prior to any implementation	users are		this purpose
28	Database Administration Training.	>=99.5% of database admin users shall be Appropriately trained prior to any implementation	>98.5%-<=99.5% of data base admin users shall be Appropriately trained prior to any implementation	<98.5% of database admin users are not Appropriately trained prior to any implementation	Monthly	• Bidder shall maintain relevant training attendance records for this purpose
29	Operating System Administration Training	>=99.5% of database admin users shall be Appropriately trained prior to any implementation	>98.5%-<=99.5% of data base admin users shall be Appropriately trained prior to any implementation	<98.5% of database admin users are not Appropriately trained prior to any implementation	Monthly	• Bidder shall maintain relevant training attendance records for this purpose
30	Critical Gaps	>=99.5%	>98.5%-	<98.5%	Daily	• Bidder shall maintain gap document

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
	Resolution Time		<=99.5%			and records for this purpose • All gaps observed in the functional specifications, current system study, training, business process re-engineering, parameterization, testing and Launch Implementation shall be resolved within defined and mutually agreed time frames.
31	Bug Reporting	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this purpose • The vendor shall ensure that all bugs reported by the users / testing team will be duly logged and assigned a unique ID for reference purposes.
32	Major Bug Resolution	<=1 calendar Day	>1-<=2 calendar days	>2 calendar days	Daily	• Bidder shall maintain relevant documents and records for this purpose
33	Medium Bug Resolution	<=3 calendar Day	>3-<=4 calendar days	>4 calendar days	Daily	• Bidder shall maintain relevant documents and records for this purpose
34	Minor Bug Resolution	<=5 calendar Day	>3-<=5 calendar days	>5 calendar days	Monthly	• Bidder shall maintain relevant documents and records for this purpose
35	Interface Identification and development	<=45 days	>45-<=60 days	>60 days	Quarterly	• The vendor will identify and develop interfaces to the existing/proposed systems so as to meet the functional

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
						requirements of the authority. The interface identification will have to done by the vendor and agreed with the IIB/IRDA within 45 days from awarding the contract.
36	Other Components (Helpdesk, networking/security components etc.)	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• The bidder will be responsible to adequately train the IRDA/IIB's personnel in Helpdesk, networking/security components and any other Components forming a part of the bidder solution.
37	Real time performance requirements – online policies issued over internet <20 seconds	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this purpose
38	Real time performance requirements – offline policies issued at insurer's office <15 minutes	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this purpose
39	Real time performance	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this

S.No.	Metric	Expected Service Level	Lower Service Level	Breach	Measurement Frequency	Measurement Method
	requirements – Claim intimation/update <30 minutes					purpose
40	Real time performance requirements – Claim finalization/settlement<30 minutes	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this purpose
	Real time performance requirements – Other reports<30 minutes	>=99.5%	>98.5%-<=99.5%	<98.5%	Daily	• Bidder shall maintain relevant documents and records for this purpose

Section 8:: Instructions/Bid related requirements

8.1. Eligibility Criteria:

This invitation of Bids is open to bidder provided they fulfill the minimum qualification criteria as mentioned below:

8.1.1. **This RFP permits submission of a single Proposal/Bid by the Bidder/Consortium.** In case of a consortium the Lead or the Partner-in-charge of the consortium designated by the members shall be the Prime Proponent/ Prime Bidder for this RFP. The Prime Proponent/Bidder should be a systems integrator and must be based in India with a registered office and should have appropriately qualified manpower employed to support this Project. The prime proponent should be duly authorized by the consortium partners to represent the consortium to the IRDA, serve as the primary contact, and take overall responsibility and accountability for performance of the work. The prime proponent, duly authorized, must become the Contractor for the purposes of Agreement negotiation and any resulting Agreement, and the consortium would be bound by the action/ inaction of the Prime Proponent. If a consortium's proposal is recommended as the Total Solution, the proponent identified as the Prime Proponent of the proposal must become the Prime Contractor for the purposes of contract negotiation, system delivery and support for the duration of the contract period. The representative of the Prime Proponent should be authorized by way of a Power of Attorney duly executed by the consortium members conferring upon the representative all powers from submission of the Proposal to negotiations and entering into Contract with IRDA. The Bidder submitting the bid will be taken as “Prime Proponent” and will be termed as ‘bidder’ for all-purposes under this RFP unless otherwise stated.

8.1.2. The bidder has to demonstrate technical competence and capabilities with reference to fraud analytics framework in the insurance sector and should have implemented similar projects (please refer to section 8.1.3) across the insurance industry in the last three years. The bidder must have a proven expertise in the financial sector specifically addressing insurance business and commit to deploy Domain Experts from the said practice to work on this Project.

8.1.3. The bidder shall have experience of having worked with other insurance regulators, insurers or organizations similar to IIB. **The bidder needs to submit satisfactory performance certificate from at least one of their clients**.

8.1.4. **The bidder should have a minimum annual turnover of Rs.250 crore each year during the last three financial years**

8.1.5. **The bidder should not have been black listed by central / state governments / Regulatory Authorities as on date of submission.**

8.1.6. Documentary proofs in support of above eligibility criteria stated above will have to be submitted with the bid.

8.2. Cost of Bidding and Proposal Preparation

The Bidder shall bear all the costs associated with the preparation and submission of its bid to IRDA/IIB. IRDA/IIB will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

8.3. Bidding Documents

The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the Bidding Documents or submission of a bid not substantially responsive to the Bidding Documents in every respect will be at the Bidder's risk and may result in the rejection of its bid without any further reference to bidder.

8.4. Supplementary Information to the RFP

At any time prior to the deadline for submission of bids, IRDA/IIB may, for any reason, modify the bidding documents by amendment at its sole discretion. Amendment in the bidding documents would be put up on the IRDA website for download. The prospective bidders, which have downloaded the bidding documents from the website of IRDA are required to provide their FAX/e-mail to IRDA at the address provided, so that amendment in the bidding documents, if any, may be notified by fax/email to all such prospective Firm/organizations. Such amendment will be binding on the prospective bidder. In order to provide, prospective Bidders, reasonable time to take the amendment into account in preparing their bid, IRDA may, at its discretion, extend the dead line for submission of bids, in such cases.

8.5. Proof of Concept

As a part of the Technical Bid, the bidders will be required to submit a proof of concept of the proposed, 'Industry wide Fraud Analytics System'. The proof of concept shall be placed before the evaluation committee for evaluation and shall form the basis for short listing of the bidder to the commercial round. It may be noted that IRDA may require the bidder to present a demonstration of the proof of concept before the evaluation committee. Bidders who fail to submit a proof of concept will not be eligible to be considered in any further bidding process. The scope of the work for the proof of the

concept will be as per the Annexure 9. The cost related to the proof of the concept shall be completely borne by the bidder.

8.6. Contents of Documents to be submitted

List of Documents Comprising the Tender Document

Sealed Cover – 1 :

- Response under Eligibility Criteria as required under clause 8 of part 1 and as per the format prescribed in Annexure 3.
- Last three years balance sheet with audited profit and loss account statements
- Power of attorney in favor of the prime proponent in case of a consortium.

Sealed Cover – 2:

The bidder shall submit the Technical Bid as per the format prescribed in Annexure 4. The following documents shall also be submitted along with the Technical Bid.

- Annexure A: Firm's/ organization's information and other relevant Information ***(in a spreadsheet)***.
- Annexure B: Acceptance of the terms and conditions and compliance of the terms mentioned in the RFP
- Annexure C: Any other documents indicating the features of services offered.
- Annexure D: Bid Earnest Money in the form of Pay Order/Demand Draft.
- Annexure E: Copies of Memorandum & Article of Association and Certificate of Incorporation.
- Annexure F: References/Testimonials from Clients where Insurance and/or Fraud solution was implemented
- Annexure G: Performance guarantee form as per the format prescribed in Annexure 5.
- Annexure H: Project Team personnel CV's as per the format prescribed in Annexure 6 and an undertaking confirming the availability of key resources for the complete project duration.
- Annexure I: Bill of Material (without cost information) as per format prescribed in Annexure 8.
- Annexure J: Proof of concept as stated in Annexure 9.
- Annexure K: Any other relevant document as deemed fit by the bidder.

Sealed Cover – 3:

Commercial Bid as per the format prescribed in Annexure 7 and Bill of Material as per the format prescribed in Annexure 8 ***(in a spreadsheet)***.

8.7. Period of Validity

Bids shall remain valid for a minimum of twelve months after the date of commercial bid opening prescribed by IRDA. A bid valid for shorter period shall be rejected by IRDA as non-responsive. Any extension in the bid validity would be for one or more periods not exceeding in total three (3) calendar months which makes total fifteen months from the date of commercial bid opening

8.8. Bid Currency

Prices shall be expressed in the Indian Rupees only.

8.9. Bidding process

8.9.1. For the purpose of the present job, a multi-stage bidding process will be followed. The response to the present tender will be submitted in three parts, Eligibility, Technical Bid and Commercial Bid. The bidder will have to submit the Technical Bid and Commercial Bid Portion of the Bids separately in sealed envelopes (wax seal), duly super scribing "TENDER FOR INDUSTRY-WIDE FRAUD ANALYTICS PROJECT" and "ELIGIBILITY", "TECHNICAL BID" or "COMMERCIAL BID" as the case may be. **Additionally, the hardcopy shall be accompanied by soft copy (in a non-rewritable CD) of the contents of the respective sealed cover**. The bidder shall invariably follow the formats prescribed in this regard.

8.9.2. TECHNICAL BID will NOT contain any pricing or commercial information at all. Technical bid with commercial information will be rejected.

8.9.3. In the first stage, eligibility criteria, would be examined. TECHNICAL BID of only those bidders who satisfy eligibility criteria will be evaluated. Those bidders satisfying the eligibility criteria and technical requirements as determined by IRDA and accepting the terms and conditions of this document shall only be short-listed. The technical bid evaluation shall also include the assessment of the POC submitted by the bidders as a part of the technical bid. Subsequent to the Technical Bid evaluation, the bidders may be asked to make a presentation before the Evaluation Committee of IRDA. The Evaluation Committee members may also visit reference site, at a mutually agreed date and the bidder should facilitate such visits by the members of Evaluation Committee.

8.9.4. In the final stage, the COMMERCIAL BID of only those bidders, whose technical bids are short listed, will be opened.

8.9.5. IRDA has the right to reject any or all the bids and IRDA's decision would be final. The bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person duly authorized

to bind the bidder to the contract. The authorization shall be indicated by written power of attorney accompanying the Bid. All pages of the bid except un-amended printed literature shall be initialed by the person(s) signing the Bid. The bid shall contain no interlineations, erasures or over writing except as necessary to correct errors made by the Bidder, in which case such corrections shall be initialed by the person(s) signing the bid.

8.10. Submission of Bids

The bidder shall duly seal each envelope with Wax Seal. The bid should be addressed to IRDA at the given address and reach on or before the date and time mentioned under Bid Details. IRDA will not be responsible for any postal delay.

8.11. Non Conforming Proposals

Any proposal may be construed as a non-conforming proposal and ineligible for consideration if it does not comply with the requirements of this RFP. The failure to comply with the technical requirements, and acknowledgment of receipt of amendments, are common causes for holding proposals as non-conforming. In addition, the IRDA will look with disfavor upon proposals that appear to be “canned” presentations of promotional materials that do not follow the format requested in this RFP or do not appear to address the particular requirements of the FAS solution, and any such bidders may also be disqualified.

8.12. Overly Elaborate Proposals

Unnecessarily elaborate brochures or other promotional materials beyond those sufficient to present a complete and effective proposal are considered undesirable and may be construed as an indication of the bidder’s lack of cost consciousness. The IRDA’s interest is purely in the quality and responsiveness of the proposal.

8.13. Language of the Proposals

The proposal and all correspondence and documents shall be written in English. All proposals and accompanying documentation will become the property of the IRDA and will not be returned. The hardcopy version will be considered as the official proposal.

8.14. Correction of errors

a. Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted will be entertained after the quotations are opened. All corrections, if any, should be initialed by the person signing the proposal form before submission, failing which the figures for such items may not be considered.

b. Arithmetic errors in proposals will be corrected as follows: In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall govern. The amount stated in the proposal form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall proposal price to rise, in which case the proposal price shall govern.

8.15. Disqualification of Proposals

IRDA may at its sole discretion and at any time during the evaluation of Proposal, disqualify any Bidder (In case of consortium primary bidder), if the Bidder has:

8.15.1. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;

8.15.2. Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years;

8.15.3. Submitted a proposal that is not accompanied by required documentation or is non-responsive;

8.15.4. Failed to provide clarifications related thereto, when sought;

8.15.5. Submitted more than one Proposal;

8.15.6. Declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices or blacklisted.

8.15.7. Submitted a proposal with price adjustment/variation provision.

8.16. Modification of Proposals

No proposal may be withdrawn in the interval between the deadline for submission of proposals and the expiration of the validity period specified by the bidder on the proposal form.

8.17. Acknowledgement of Understanding of Terms

By submitting a proposal, each bidder shall be deemed to acknowledge that it has carefully read all sections of this RFP, including all forms, schedules and annexures hereto, and has fully informed itself as to all existing conditions and limitations.

8.18. Terms and Conditions

8.18.1. IRDA expects the bidding parties /bidders to adhere to the terms of this RFP and would not accept any deviations to the same. If the bidding parties/bidders have absolutely genuine issues only then should they provide their nature of non – compliance to the same. IRDA shall consider the non compliance and shall at its own discretion accept or reject the deviations. IRDA reserves its right to not accept such deviations to the tender terms and in that case the bidding party/bidder (primary bidder in case of consortium) shall be bound to comply with the terms. Any noncompliance would be treated as a breach and shall invoke Liquidated Damages.

8.18.2. Unless expressly overridden by the specific agreement to be entered into between IRDA and the bidding party/bidder (primary bidder in case of consortium), the RFP shall be the governing document for arrangement between IRDA and the bidding party/bidder (primary bidder in case of consortium)s. Any additional or different terms and conditions proposed by the bidding party/bidder (primary bidder in case of consortium) would be rejected unless expressly assented to in writing by IRDA. Decision of IRDA shall be final and binding.

8.18.3. Responses to this RFP should not be construed as an obligation on the part of IRDA to award a contract for any services or combination of services. Failure of IRDA to select a bidding party/bidder (primary bidder in case of consortium) shall not result in any claim whatsoever against IRDA and IRDA reserves the right to reject any or all proposals in part or in full, without assigning any reason whatsoever.

8.18.4. By submitting a proposal, the bidding party/bidder (primary bidder in case of consortium) agrees to promptly contract with IRDA for any work awarded to the bidding party/bidder (primary bidder in case of consortium). Failure on the part of the awarded bidding party/bidder (primary bidder in case of consortium) to execute a valid contract with IRDA will lead to the forfeiture of the Earnest Money Deposit (EMD) and relieve IRDA of any obligation to the bidding party/bidder (primary bidder in case of consortium), and a different bidding party/bidder (primary bidder in case of consortium) may be selected.

8.18.5. The bidding party/bidder (primary bidder in case of consortium) must strictly adhere to the delivery dates or lead times identified in their proposal. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to IRDA, may constitute a material breach of the bidding party/bidder (primary bidder in case of consortium)'s performance and attract Liquidated Damages. In the event that IRDA is forced to cancel an awarded contract (relative to

this RFP) due to the bidding party/bidder (primary bidder in case of consortium)'s inability to meet the established delivery dates, the bidding party/bidder (primary bidder in case of consortium) shall be responsible for payment of 200% of the costs incurred by IRDA for re-procurement of such undelivered goods or services. The liability in such an event could be limited to the value of the contract. In addition to this the bidding party/bidder (primary bidder in case of consortium) shall also be liable to the liquidated damages as may be fixed by IRDA.

8.18.6. The bidding party/bidder (primary bidder in case of consortium) also acknowledges that IRDA relies on this statement of fact, therefore neither accepting responsibility for, nor relieving the bidding party/bidder (primary bidder in case of consortium) of responsibility for the performance of all provisions and terms and conditions of this RFP, IRDA expects the bidding party/bidder (primary bidder in case of consortium) to fulfill all the terms and conditions of this RFP.

8.18.7. The bidding party/bidder (primary bidder in case of consortium) represents that the proposed software solution and its documentation and/or use of the same by IRDA shall not violate or infringe the rights of any third party or the laws or regulations under any governmental or judicial authority. The bidding party/bidder (primary bidder in case of consortium) further represents that the documentation to be provided to IRDA shall contain a complete and accurate description of the software and services (as applicable), and shall be prepared and maintained in accordance with the highest industry standards. The bidding party/bidder (primary bidder in case of consortium) represents and undertakes to obtain and maintain validity throughout the project, of all appropriate registrations permissions and approvals, which are statutorily required to be obtained by the bidding party/bidder (primary bidder in case of consortium) for performance of the obligations of the bidding party/bidder (primary bidder in case of consortium). The bidding party/bidder (primary bidder in case of consortium) further undertakes to inform and assist IRDA for procuring any registrations, permissions or approvals, which may at any time during the Contract Period be statutorily required to be obtained by IRDA for availing services from the bidding party/bidder (primary bidder in case of consortium).

8.18.8. The bidding party/bidder (primary bidder in case of consortium) undertakes to provide appropriate and trained human as well as other resources required, to execute the various tasks assigned as part of the project, from time to time.

8.18.9. IRDA would not assume any expenses incurred by the bidding party/bidder (primary bidder in case of consortium) in preparation of the response to this RFP and also would not return the bid documents to the bidding party/bidder (primary bidder in case of consortium)

8.18.10. IRDA shall not be held liable for costs incurred during any negotiations on proposals or proposed contracts or for any work performed in connection therewith.

8.18.11. The bidding party/bidder (primary bidder in case of consortium) shall be responsible for managing the activities of its personnel and will be accountable for both. The bidding party/bidder (primary bidder in case of consortium) shall be liable for any acts, deeds or things done by their employees, agents, etc. which is outside the scope of power vested or instructions issued by IRDA. bidding party/bidder (primary bidder in case of consortium) shall be the principal employer of the employees, agents, etc. engaged by bidding party/bidder (primary bidder in case of consortium) and shall be liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under the contract to be issued for this tender.

8.18.12. In no event IRDA shall be the employer of the employees, agents, etc. engaged by bidding party/bidder (primary bidder in case of consortium). No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, etc. by the bidding party/bidder (primary bidder in case of consortium), for any assignment under the contract to be issued for this tender. All remuneration, claims, wages, dues etc. of such employees, agents, etc. of bidding party/bidder (primary bidder in case of consortium) shall be paid by bidding party/bidder (primary bidder in case of consortium) alone and IRDA shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of bidding party/bidder (primary bidder in case of consortium)'s employee, agents, . The bidding party/bidder (primary bidder in case of consortium) shall hold IRDA, its successors, Assignees and Administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to IRDA through the action of its employees, agents, etc. However, the bidding party/bidder (primary bidder in case of consortium) would be given an opportunity to be heard by IRDA prior to making of a decision in respect of such loss or damage.

8.18.13. IRDA shall inform the bidding party/bidder (primary bidder in case of consortium) all breaches and claims of indemnification and shall grant the bidding party/bidder (primary bidder in case of consortium) sole authority to defend, manage, negotiate or settle such claims; and make available all reasonable assistance in defending the claims (at the expense of the bidding party/bidder (primary bidder in case of consortium)).

8.18.14. The bidding party/bidder (primary bidder in case of consortium)'s representative and local India office will be the contact point for IRDA

8.18.15. Bidding party/bidder (primary bidder in case of consortium) should ensure that the hardware delivered to IRDA including all components and attachments are brand new and the software delivered is the latest released version. In case of software supplied with the system, the bidding party/bidder (primary bidder in case of consortium) should ensure that the same is licensed and legally obtained with valid documentation made available to IRDA/IIB

8.18.16. The bidding party/bidder (primary bidder in case of consortium) shall procure in the name of IRDA all user specific software licenses for IRDA, based on number of CPUs at the Data Centre and Disaster Recovery site. Bidding party/bidder (primary bidder in case of consortium) shall also provide other licenses for applications, operating system and database as required by IRDA to successfully utilize the solution. The bidding party/bidder (primary bidder in case of consortium) shall provide the licenses for all software being a part of its proposed solution to IRDA/IIB.

8.18.17. The bidding party/bidder (primary bidder in case of consortium) shall ensure that the solution provided and sized by the bidding party/bidder (primary bidder in case of consortium) is capable of meeting IRDA's current and future transaction and business volumes. Empirical evidence of the appropriateness of the server sizing by means of comparison with benchmarked data on a similar environment as proposed to IRDA/IIB will be mandatory.

8.18.18. The bidding party/bidder (primary bidder in case of consortium) shall perform the services and carry out its obligations under the contract with due diligence and efficiency, in accordance with generally accepted techniques and practices used in the industry and with professional engineering and training/consulting standards recognized by national/international professional bodies and shall observe sound management, technical and engineering practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods. The bidding party/bidder (primary bidder in case of consortium) shall always act, support and safeguard IRDA's legitimate interests in any dealings with third parties.

8.18.19. Project Team: IRDA will interview the proposed team members of bidder who will be working in this project. Once selected, the team members cannot be changed without prior approval of IRDA. However, IRDA will have the right to ask the bidder to replace a team member, if that person is not found to be equipped with the required skill, during the course of the project.

8.19. Bid Earnest money/EMD

The bidder have to submit the Bid Earnest Money/EMD of Rs.10,00,000/-(Rs. Ten lakhs Only) in the form of Demand Draft/ Pay Order/Bank Guarantee favouring: 'Insurance Regulatory and Development Authority' and payable at Hyderabad at the time of submission of the bid documents. In absence of Earnest Money, bid will be rejected. EMD of unsuccessful bidder will be refunded within 45 days from the date of opening of commercial bid. EMD of the successful bidder will be refunded within one month after signing of contract and submission of Performance Bank Guarantee for 10% of the total cost of project. IRDA/IIB will not pay any interest on the EMD amount.

Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event the IRDA shall forfeit the EMD amount and blacklist the bidder to be considered for any future assignments at a later point in time.

The earnest money deposit (EMD) may also be forfeited:

- If the bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid Form
- If the bidder does not accept the correction of its Bid
- In the case of a successful bidder, if the bidder fails within the specified time limit to sign the Contract Agreement, or to furnish the required performance guarantee
- If the bidder fails to produce sufficient proof for the information provided as part of response of technical bid evaluation.

8.20. Venue & Deadline for submission of proposals

Bid must be received by IRDA at the address specified in Bid Document not later than the specified date and time as specified in Bid Document. In event of the specified date for submission of bids being declared a holiday for IRDA, the bids will be received up to appointed time on next working day. IRDA may, at its discretion, extend this deadline for submission of bids by amending the bid, in which case all rights and obligations of IRDA and bidder previously subject to the deadline will thereafter be subject to the deadline as extended.

Proposals must be submitted physically and put inside tender box available at the following address:

Shri Randip Singh Jagpal,
Joint Director,
Insurance Regulatory and Development Authority,
3rd floor, Parisrama Bhavan,
Basher Bagh, Hyderabad – 500 004

8.21. Last Date & Time of submission:

Proposals must be submitted before or by 1500 hours on the last date given at Key Activities and Dates section. IRDA may, under exceptional circumstances and at its sole discretion, extend the deadline for submission of proposals by issuing a notice and this information will be made available in the website (http://IRDA.gov.in) and will be binding to all. All rights and obligations of the FAS project and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

8.22. Late Bids

Any bid received by IRDA after the deadline for submission of bid will be summarily rejected and/or returned unopened to the bidder, if bidder desired so, against proper receipt.

8.23. Modifications and Withdrawal

Bids once submitted will be treated, as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids. In case of successful bidder, he will not be allowed to withdraw/back out from the bid commitments. The bid earnest money in such eventuality shall be forfeited and all interests/claims of such bidder shall be deemed as foreclosed.

8.24. Bid Opening and Evaluation

8.24.1. IRDA will open the bids, in the presence of bidder representative who chooses to attend, at the time and date mentioned in Bid document at the address mentioned in Para "Submission of Bids". The bidder representatives who are present shall sign register evidencing their attendance.

8.24.2. Failure to demonstrate to the satisfaction of IRDA on the working of the solution in Insurance sector will be treated as not fulfilling all the terms and conditions of RFP and will make the bid liable to be rejected. The decision of IRDA will be final and no correspondence will be entertained in this regard. IRDA reserves the right to reject any and all proposals without assigning any reason. IRDA will scrutinise the offers received to determine whether they are complete as per RFP requirement, whether technical documentation as asked for and required to evaluate the offer has been submitted and whether the documents have been properly signed. IRDA may, at its discretion, waive any minor non-conformity or any minor irregularity in the offer. This waiver shall be binding on all the Bidders and IRDA reserves the right for such waivers.

8.24.3. It may be noted that this document provides details about what should be in the solution but the evaluation committee will be very receptive to alternatives which can lead to better results and significantly lower costs.

8.24.4. Only those bidders who satisfy the 'eligibility criteria' will be shortlisted for the technical evaluation

8.24.5. IRDA may choose to invite the bidders to discuss and clarify their technical proposal. Any change in the proposal, however, shall not be permissible after the bid submission. IRDA reserves the

right to accept or reject any bid or to annul the bidding process and reject all bids at any time prior to the award of contract, without thereby incurring any liability to the affected bidders; without giving any reasons whatsoever.

8.24.6. Technical Bids to the RFP would be evaluated on the technical criteria set below by assigning the relevant scoring on each of the technical parameters. Technical bids shall be opened and evaluated for acceptability of the techno-functional requirements, deviations and other technical suitability. The Bidders shall respond to the requirements as per the Forms and Data templates requested in this document. The bidders will be required to present their proposal to the IRDA Technical Committee. The technical evaluation would be carried out on the following parameters and associated weights thereof are as given below:

Sl.No.	Technical Evaluation Criteria	Weightage
1	Firm's/ Organization's responsiveness and understanding of requirements	10
2	Solution Architecture Proposed (including Software and Hardware) and fit between functional and technical requirements.	20
3	Previous Experience of similar nature and record of accomplishment based on competency & expertise of key personnel earmarked for this assignment	10
4	Proof of Concept	15
5	Technical Presentation	10
6	Level of compliance with contractual terms	10
7	Implementation approach/methodology and time schedule	15
8	Quality Assurance Mechanism and Site Visits	10

Each of these data fields (information category defined above) have been detailed out with their specific metrics, their scoring methodology and specific information, as given in their respective forms. The score against each of these information categories shall be calculated as below:

Score on a data field = Total score achieved/ Maximum score achievable * Weightage of the respective data field. No score shall be awarded against any forms, items and data fields where the relevant information is not provided.

8.24.7.

(a) The commercial bids of all bidders who score a minimum of 60% in technical evaluation and any bidder within the range of 15% score of the top bidder shall be considered. And, in an event where any bidder within the range of 15% score of the top bidder scores less than 60%, all such

bidders within the range of 15% score of the top bidder fulfilling a minimum score of 50% on technical evaluation shall also be considered.

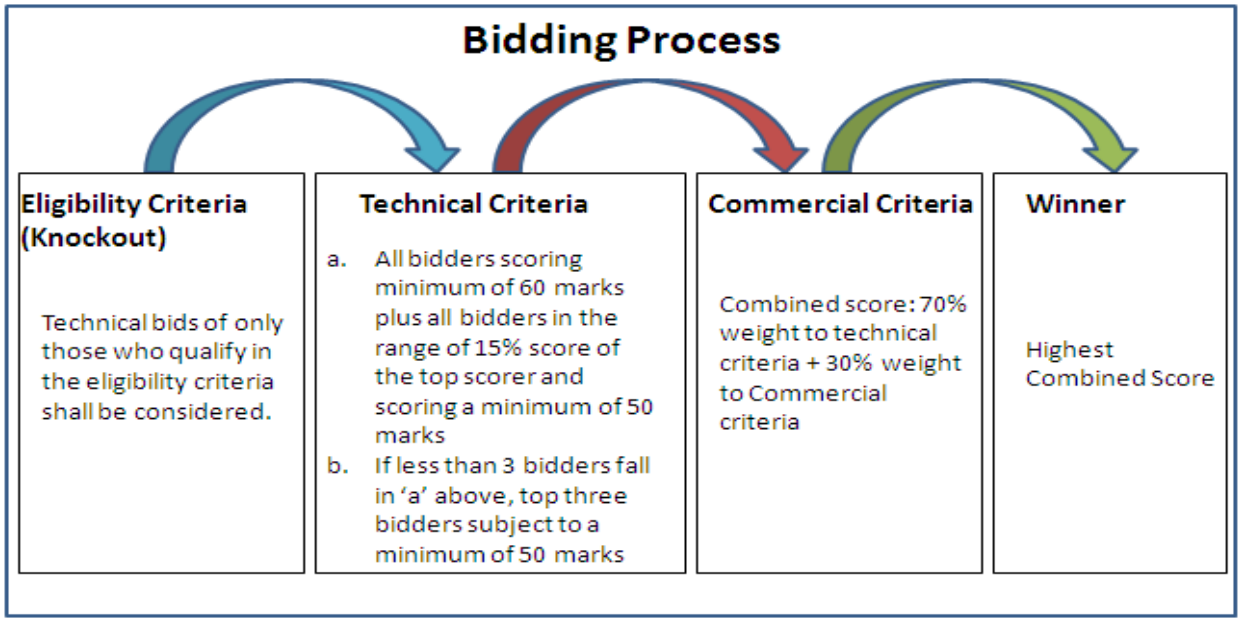
(b) In an event where there are less than three bidders as per the criteria (a) above, commercial bids of top three bidders fulfilling minimum of 50% score on technical evaluation shall be considered.

8.24.8. Technical score:. The technical proposal of the bidder getting the highest marks will be ranked as T-1 and the next highest will be ranked as T-2, T-3, etc., IRDA may choose to invite the firm/ organization to discuss and clarify their technical proposal. Any change in the proposal, however, shall not be permissible after the bid submission.

8.24.9. The commercial bid shall be opened in the presence of Bidders' representative, whose bids are considered as responsive as per the technical and other qualification criteria as underlined in the bid document. The intimation of time and place of opening of commercial bids will be informed separately to successful bidder(s) only. Commercial bid with the lowest cost will be given a financial score of 100 and other proposals will be given a financial score that is inversely proportional to their price. Subsequent to the price bid evaluation, the successful Bidder shall be issued a letter of intent as per specified timelines. The bidder shall furnish the performance guarantee as per the attached format within two weeks of the receipt of the letter of intent. The Authority reserves the right to satisfy itself of the reasonability of the commercial bid in all aspects.

8.24.10. The technical proposal will be allotted a weightage of 70% while the commercial bid will be allotted a weightage of 30%

8.24.11. The total score, both of the technical and commercial shall be obtained by weighing the technical and commercial bid as above and aggregating the same. On the basis of the combined weighted score for technical and commercial bid, the bidders will be ranked in terms of the total score obtained. The proposal obtaining the highest total combined score will be ranked as H-1 and the next highest will be ranked as H-2, H-3, etc. The bidder securing the highest combined marks and ranked H-1 will be identified and invited for negotiations. Diagrammatic representation of the bidding process is as follows. This is followed by examples of selection methodology.



EXAMPLES OF SELECTION METHODOLOGY

Example 1:

As an example, the following procedure will be followed. The weightage of the technical bids and financial bids is kept as 70:30. In response to the RFP, say 4 proposals, A,B,C & D were received. **The technical evaluation committee awarded them 90, 80, 75 and 59 marks for the technical bid respectively, thereby ranking them as T-1, T-2, T- 3 and T-4 respectively**.

The financial proposals of top three technically ranked bidders, i.e. T-1, T-2 and T-3 were only opened as the fourth bidder who scored 59 marks was not within the range of 15% score of the top scorer.

The evaluation committee examined the financial proposals and evaluated the quoted prices as under:

Proposal	Evaluated Cost
A	Rs.120
B	Rs. 100
C	Rs.110

Using the formula LEC / EC, where LEC stands for lowest evaluated cost and EC stands for evaluated cost, the committee gave them the following points (rounded to nearest two decimal places) for financial proposals:

A : 100 / 120 = 83.33 points
B : 100 / 100 = 100.00 points
C : 100 / 110 = 90.91 points

In the combined evaluation, thereafter, the evaluation committee calculated the combined technical and financial score as under:

Proposal A: 90x0.70 + 83.33x0.30 = 88.00 points.
Proposal B: 80x0.70 + 100.00x0.30 = 86.00 points
Proposal C: 75x0.70 + 90.91x0.30 = 79.77 points.

The three proposals in the combined technical and financial evaluation were ranked as under:

Proposal A: 88.00 points : H-1
Proposal B: 86.00 points : H-2
Proposal C: 79.77 points : H-3

Proposal A at the evaluated cost of Rs.120 was, therefore, declared as winner and recommended for negotiations/approval, to the competent authority.

Example 2:

As another example, the technical evaluation committee awarded the bidders, 86, 82, 80, 78, 75,70 and 59 marks for the technical bid respectively. These bidders are as such ranked as T-1, to T-7 respectively. Short listing of bidders on the technical scoring will be done as follows:

All who scored minimum of 60 marks include bidders scoring 86, 82, 80,78, 75,70. Bidders within 15% score of the top scorer are those scoring: 85, 82, 80, 78, 75 marks (86*85%)

All bidders who scored minimum of 60% (86, 82, 80,78, 75,70) will be shortlisted and their commercial bids shall be opened. The combined score, H1 bidder shall then be determined as per the example 1 above.

The contract shall be awarded to the responsible, responsive bidder whose proposal conforms to the RFP and in the opinion of IRDA/IIB, represents the best value to the project, as per the evaluation procedure prescribed above.

Example 3:

As another example, the technical evaluation committee awarded the bidders, 62, 59 and 51 marks for the technical bid respectively. These bidders are as such ranked as T-1, to T-3 respectively. Short listing of bidders on the technical scoring will be done as follows:

a. All who scored minimum of 60 marks include bidders scoring 62. Bidders within 15% score of the top scorer are those scoring: 62, 59 (62*85%)

b. Since less than 3 bidders qualified under 'a' above, top three bidders scoring a minimum of 50 marks with scores of 62, 59 and 51 will be shortlisted and their commercial bids shall be opened. The combined score, H1 bidder shall then be determined as per the example 1 above.

The contract shall be awarded to the responsible, responsive bidder whose proposal conforms to the RFP and in the opinion of IRDA/IIB, represents the best value to the project, as per the evaluation procedure prescribed above.

8.25. Clarifications on Bidder Enquiries and IRDA Responses and Contact Person

To assist in the examination, evaluation and comparison of bids IRDA may, at its discretion, ask the firm/ organization for clarification, presentation, and response in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

A bidder requiring any clarification of the bidding documents may notify IRDA in writing or by fax. IRDA will respond in writing to any request for clarifications which it receives not later than 16-01-2013. Any questions concerning this RFP must be submitted in writing on or before the last date for clarifications to:

Shri Randip Singh Jagpal, Joint Director (Non-Life),Insurance Regulatory and Development Authority, 3rd floor, Parisrama Bhavanam, Basher Bagh, Hyderabad – 500 004 Phone: 91-40-23210164 Email: randip@irda.gov.in. Similarly, the Bidder should nominate a person as a single point of contact from within its organisation. The name, postal address, e-mail address and contact phone numbers of such person should be mentioned in the proposal. No requests for clarification will be entertained by telephone or in person. If a bidder discovers any significant ambiguity, error, conflict, discrepancy, omission or other deficiency in this RFP, the bidder should immediately notify to the above official of such error and request modification or clarification of the RFP document, which modification/clarification shall be provided at the sole discretion of IRDA.

8.26. Rejection of a bid

IRDA's decision to reject a bid and forfeit the EMD will be final and without prejudice and will be binding on all parties.

8.27. IRDA's Right to Terminate the Process

The IRDA may terminate the RFP process at any time and without assigning any reason. The IRDA makes no commitments, express or implied, that this process will result in a business transaction with anyone. This RFP does not constitute an offer by the IRDA. The bidder's participation in this process may result in IRDA selecting the bidder to engage in further discussions and negotiations toward execution of a contract. The commencement of such negotiations does not, however, signify a commitment by IRDA to execute a contract or to continue negotiations. The IRDA may terminate negotiations at any time without assigning any reason.

8.28. Key Activities and Dates

S.No	Activity	Date
1	Issue of RFP	04/12/2013
2	Pre-bid conference	18/12/2013
3	Last date for submission of pre-bid queries	24/12/2013
4	Posting of replies to pre-bid queries	15/01/2014
5	Publishing Final RFP by IRDA	05/02/2014
6	Last Date for submission of Bids	02/04/2014 at 15:00 hours
7	Opening of Eligibility Criteria – Sealed Cover -1	02/04/2014 at 16:30 hours
8	Opening of Technical Bids	09/04/2014 at 16:30 hours
9	POC and Technical Presentations	16/04/2014 onwards
10	Announcement of shortlisted bidders who qualify for Commercial bidding round	25/06/2014
11	Date of Commercial Bid opening	02/07/2014

8.29. Award

8.29.1. The contract will be awarded to the responsible, responsive bidder whose proposal conforms to the complete RFP (parts 1, 2 and all annexure documents) and, in the opinion of the IRDA, represents the best value to the FAS project, as per the evaluation procedure prescribed in the RFP.

8.29.2. The successful bidder shall be invited to do a detailed presentation giving the solution approach covering the following:

- Justification for the commercials quoted with a detailed statement of work and hardware/software solutions including sizing of the solutions.
- Mapping of the solutions, both hardware and software, to the business and technical requirements item-wise and the rationale for choosing the solution suggested (For example, a solution may work in one kind of environment)

IRDA/IIB reserves the right to negotiate the contract price and to modify the stack where the business or/and Technical requirements can be better met with the modification mutually agreed.

8.29.3. **IRDA's right to accept any Proposal and to reject any or All Proposals**

IRDA reserves the right to accept or reject any proposal, and to annul the tendering process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for IRDA's action.

8.29.4. **Notification of Award**

Prior to the expiration of the validity period, IRDA will notify the successful bidder in writing or by fax or email, to be confirmed in writing by letter, that its proposal has been accepted. The notification of award will constitute the formation of the contract. Upon the successful bidder's furnishing of performance bank guarantee, IRDA will notify each unsuccessful bidder.

8.29.5. **Signing of Contract**

The bidder (prime bidder in case of consortium) shall sign the agreement with IRDA in the format in alignment with TCRFP of this RFP and as discussed and agreed between the Bidder and IRDA/IIB at the time of award of the contract, within 60 days of the award or within such extended period as may be specified by IRDA. The agreement shall include system & procedure to be adopted by bidder as desired by IRDA. The Firm/organization is also required to enter into a Non-Disclosure Agreement with IRDA for confidentiality/secrecy of data/system and processes. IRDA reserves its right to modify any clause of the agreement prior to signing and upon adequate notice to the bidder. Non-fulfillment of this condition of executing a contract by the successful bidder within the specified period would constitute sufficient ground for annulment of the award and forfeiture of Bid Earnest Money.

8.29.6. **Performance Bank Guarantee**

- The successful bidder shall at his own expense deposit with IRDA, within 21 days of the date of notice of award of the contract or prior to signing of the contract whichever is earlier, an unconditional and irrevocable Performance Bank Guarantee (PBG) from a scheduled bank acceptable to IRDA, payable on demand, for the due performance and fulfillment of the contract by the bidder. The PBG will be made in the format given at Annexure 5.

- This shall be for 10% of the total project cost and for a minimum period until:

    - Two years from the date of expiry of the contract or
    - Two years from earlier termination of the contract

In case, IRDA/IIB decides to extend the contract at the discretion of IRDA/IIB, the performance bank guarantee shall be extended for a minimum period until two years from the expiry of such extended period. Failure of the successful bidder to comply with the requirement shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security (EMD), in which event IRDA may make the award to the next eligible bidder.