Annexure 15- Technical Specifications - Scoring Sheet

Instructions of Filling up of Annexure 15

1 "S.No." - Serial Number of the Requirement Provided by the OICL. Bidder must not change any information in this column

2 "Particulars" - The detailed Requirement. Bidder must not change any information in this column.

3 "BC" - Bidder's Compliance – Bidder would be required to provide an appropriate score to each requirement requested for as per the following Table

BC	Description
Yes	Bidder's solution complies to this and/or provides this feature.
No	Bidder's solution does not comply to this and/or does not provide this feature.

4 Marks for specifications for will be allotted against the responses to each of the point mentioned as per the following marking pattern:

Scale	Description
10	Yes
0	No

5 Sheets will be scored on Yes/No compliance by the bidder. Yes/No responses will be marked as per the above table.

6 Each line item in the technical specifications sheet mentioned in Annexure 15 carries 10 marks. The marks allotted to the responses of the Bidder by the OICL, would be reduced to a scale proportionate to the marks allocated for the technical evaluation. It is important for the bidder to score 100% marks in Technical Specifications.

Notes

1	Bidder is expected to provide for all requirements irrespective of the functionality of the solution proposed. Hence the overall cost must include all the requirements where the rank provided is Yes or NO. However, for line items marked as "No", the OICL at its discretion may undertake a normalization exercise and conclude accordingly.
2	In case the Bidder fails to provide a " Bidder Compliance" against any of the line items the response would be considered as incomplete and may not be scored, at OICL's discretion
3	Bidder is expected to provide the response by filling up the columns "Bidder' Compliance (BC)" and "Bidder Remarks" only. Bidder is advised not to make any changes to any information on the RFP documents for example insert a row or delete a row or modify any other information like change the functionality required, etc.
4	Every requirement needs to be treated as an individual requirement and should not be clubbed with any other requirement and the Bidder needs to provide a "Bidder's Compliance" for that individual requirement, in case the Bidder clubs the requirements the response would be treated as incorrect .
5	The Evaluation Committee decided by the OICL would be marking this annexure already scored by the bidder and would be appropriately assigning the final marks. The OICL will have the discretion to change the marks against the Bidder's scored line item if the bidder/OEM is not able to showcase the same in Product walkthrough or Presentation.
6	The marks allotted to the responses of the Bidder by the OICL after carrying out the above steps above would be reduced to a scale proportionate to the marks allocated for the functional & technical evaluation for the respective module. It is important for the bidder to score 100% of the marks for Technical Specifications.
7	Bidder to note that this is a minimum requirement specifications and the bidder is required to size and propose as per solution requirement considering the growth for the entire duration of the contract
8	Bidder is free to use virtualization as per requirement and compatibility with the solution; in case of virtualization is proposed bidder is required to ensure the security and automation of virtual environment with centralized dashboard for monitoring and management.
9	Bidder is free to choose the server compute hardware either RISC / EPIC or X86 in line with the solution architecture and required for successful implementation and sustainance of the solution for the tenure of the contract adhering SLA requirement. Bidder is required to keep a vertical headroom of 30% within the server and 30% withing the chassis.

S.No.	Particulars		Bidder' s Compliance (Yes/No)	Bidder's Remarks
1	**Existing functionalities**			
1.1	**General Functions**			
1.1.1	INLIAS (OICL Core Insurance Software)	The Portal works with high level SOA based integration with core insurance business application (INLIAS).		
1.1.2	Online Policy Issuance from Portal	For every business transaction the Portal interacts with the existing core application and database. Actual process is done in INLIAS and policy is issued from INLIAS on Portal request. Required Data capturing is allowed in Portal for such transaction.		
		Policies issued against payment through payment gateway using Credit card/ Debit card/Internet banking. Softcopy of policy document/certificate is sent to e-mail ID only.		
		Retry of generation of policy for failed transaction after successful payment process is enabled.		
1.1.3	Claim Intimation acceptance from Portal	Portal accepts the required details and interacts with INLIAS for acceptance of Intimation.		
		It triggers email/SMS alert to customer / Centralized Service Center with Claim No. generated from Core application		
1.1.4	Queries like Policy Status and Claim Status, etc.	Some of the Straight thru queries are requested directly from the INLIAS database. These queries are served through integration layer. Portal does not access directly the Core database.		
1.1.5	Data updation from INLIAS Database	Updation of data from INLIAS in real-time or in a batch, if required as per the design requirement of Portal database.		
1.1.6	Online Portal transaction trigger based Data updation from Portal Database to INLIAS Database	Whenever a transaction take place in Portal the details (as per the INLIAS record set requirement) are sent to INLIAS database for synchronization.		
1.1.7	SMS and E-Mail Alerts	Integration with the SMS (Short Messaging Service) to send SMSs programmable on events. SMS Push API Method. SMS events (transactional) for INLIAS and Portal has been configured by SMS Integrator. Presently Sender ID is OICLIN for SMS Templates of our core insurance solution INLIAS. Sender ID is OICWEB for SMS Templates of our Web Portal www.orientalinsurance.org.in. Marketing department is also availing the services of SMS Integrator.		
1.1.8	Integrated Grievance Management System (IGMS) of IRDA	Integration of the Portal with Integrated Grievance Management system (IGMS) of IRDA including the provision for batch upload/download (Web Services + Batch Upload). Web services to integrate and synchronize our grievance data online with IGMS and/or synchronize complaint's Data with IGMS by Batch Upload facility.		

1.1.9	Bill desk Payment Gateway	Integration of the Portal with Bill desk Payment Gateway integration and payment reversal process. It facilitates online electronic payment services (through Net Banking, Debit Cards and Credit Cards of multiple Banks) through the OICL's Portal.		
1.1.10	GI Council for OMP Verifications	Online verification of Overseas Mediclaim Policies issued by our Company. An URL of Oriental Insurance has been provided to General Insurance Council of India (http://www.gicouncil.in) for querying and verifying the authenticity of Overseas Mediclaim Policy (OMP) particulars submitted by a person seeking Visa from Schengen states. Web services has been developed by 3i-Infotech for the same. The OICL Portal (developed by PWC) will invoke the INLIAS web service with the Policy Number or Passport Number parameters. The INLIAS web service will send back the following information which will be used by Portal system:		
		1. Insured Name		
		2. Policy Start Date		
		3. Policy End Date		
		4. Passport Number		
		5. Sum Insured		
		6. Policy Status		
1.1.11	Mobile Point of Sale (MPOS)	Integration of MPOS devices (For Ezeetap V2) from Yes Bank with OICL's Mobile Application. These devices are attached to Smart Phones with Android Operating System. Using This device Agents will Swipe the Credit Card/ Debit Card of the Customer for collecting the Renewal premiums.		
1.1.12	Offline Policy Creation	Provision For creating Policies Offline against Failed Attempts on Web Portal		
1.1.13	ICAI Discount on Web Portal	Enablement of discount of 55% on OD premium (Motor Policies) for 2 wheelers and 4 wheelers for members of ICAI in web portal.		
1.1.14	Enablement on Portal	Enablement of an option to login to portal for Employees with designation Development Officer (DO); Admn.Off.(D); Divl.I/c; Br.I/c; Asstt.Mgr.(D); and Agency Manager can access OICL Portal as agents and view a dashboard similar to that of agents with separate credentials in Web Portal.		
1.2	Mobile access	The mobile version of the Portal is accessible and compatible with major mobile browsers . Policies of "Oriental" can also be renewed online through WAP enabled mobile phones by visiting http://m.orientalinsurance.org.in. Integration of our Web Portal with mobile WAP browser based application for the customers and Agents. Short code based integration with the SMS gateway is integral part of the mobile application.		

1.3	Online Policy Selling	The portal allows the customer to buy certain products from OICL. Selling of policies through portal is presently cover the following insurance segments. Appropriate access, authorization and security controls are incorporated into the Portal system.		
1.3.1	Health	Individual Mediclaim, Happy family floater policy		
1.3.2	Personal Accidents	Personal Accident Policy, Janata Personal Accident Policy		
1.3.3	Travel	Overseas Mediclaim Policy		
1.3.4	Motor	Package policy for Private Car and Motor Cycle		
1.3.5	Shop Keepers	Shop Keepers Policy		
1.3.6	Home	Householders Insurance Policy		
1.3.7	Nagarik Surksha	Nagarik Suraksha Policy		
1.4	Online Policy Renewals	The portal allows the user to renew all the policies of OICL and allows the user to renew the Motor insurance policy and Personal Accident policy from the other General Insurance Companies.		
1.4.1	Renewals of OICL policies	The Portal allows to renew existing policies of OICL.		
1.4.2	Renewals other than OICL policies	The Portal also allows to renew the policies Motor Insurance Policy and Personal Accident Policy from the other General insurance companies.		
1.5	Customers Portal	Existing customers of OICL should be able to register in portal and view the customer specific details.		
1.5.1	Edit profile	The Customers are allowed to edit their profile on our Portal		
1.5.2	Change password	The customers are able to change their password if they want		
1.5.3	Home	The customers home page contains the list of policies, list of claims, list of expired policies, claims status with TPA and alerts related to policies which are going to expire.		
1.5.4	Buy a new policy online	The customer is able to buy all the new products specified in section 3		
1.5.5	Renew the existing policy of OICL	The customer is able to renew all the policies specified in section 4 of OICL		
1.5.6	Renew the existing policies of companies other than OICL	The customer is able to renew the motor policy and personal accident policy from the companies other than OICL		
1.5.7	Policy Schedule Request	Image of the Policy Schedules is stored in a server and on request from the customer is sent via Email only. The archival can be based on Policy Number and Insured Name (Customer Name) and other details.		
		Policy Schedule is generated from INLIAS as PDF document.		
1.5.8	View saved proposals	The customers are able to view the saved proposals related to policies.		
1.5.9	Claims	Customer is able to intimate a claim against his existing policy with required details. Once a claim successfully accepted by portal the details are sent to INLIAS database for updation and claim intimation number generation.		

		This may trigger an alert to the Office concerned/service center/customer. The customer can also view his already intimated claims and status.		
1.5.10	Policy Registration	The customer can register their policy on portal.		
1.5.11	Marine Declaration	The customer can able to view his marine declarations		
1.5.12	Register Grievance	The customer can register the Grievance.		
1.5.13	Search Grievances	The portal allows the customer to search the grievances		
1.5.14	View Transactions	The customer can view his transactions history		
1.6	Corporate Customer			
1.6.1	Edit profile	The portal is able to edit the information of the corporate customer		
1.6.2	Change password	The corporate customers can change their password if they want		
1.6.3	Home	The corporate customers home page contains the list of policies, list of claims, list of expired policies and claims status with TPA.Their home page should display customized contents for cross/up selling and certain broadcast messages(if any)		
1.6.4	Buy a new policy online	The corporate customer can buy all the new products specified in section 3		
1.6.5	Renew the existing policy of OICL	The corporate customer can renew all the policies specified in section 4 of OICL		
1.6.6	Renew the existing policies of companies other than OICL	The corporate customer can renew the motor policy from the companies other than OICL		
1.6.7	View saved proposals	The corporate customers are able to view the saved proposals related to policies.		
1.6.8	CD Account	Cash Deposit (CD) Balance and status is shown for specific corporate customers.		
		Details have to be fetched from INLIAS.		
1.6.9	Search Claims	All reported claims and status are available on request for the corporate customer.		
		Details have to be fetched from INLIAS.		
1.6.10	Claims	Corporate Customer is able to intimate a claim against his existing policy with required details. Once a claim successfully accepted by portal the details are sent to INLIAS database for updation and claim intimation number generation.		
		This may trigger an alert to the Office concerned/service center/customer. The customer can also view his already intimated claims.		
1.6.11	Marine Declaration	The corporate customer can able to view his marine declarations		
1.6.12	Register Grievance	The corporate customer can register the Grievance.		
1.6.13	Search Grievances	The portal allows the corporate customer to search the grievances		
1.6.14	Bulk Upload of proposal data (OMP, Motor) in specified format for issuance of	Uploading facility for batch policy for limited number of data in a specified format.		
		The file in a specific format is allowed from the specific corporate customer and from Portal the file is sent to INLIAS for processing.		

1.6.14	Motor) in specified format for issuance of policy and processing.	Portal acts as an intermediate media in this case. The corporate customer can able to create bulk policies, Open declaration generation and risk uploading and he can download the document templates.		
1.6.15	View Transactions	The corporate customer can view his transactions history		
1.7	Agents Portal	Comprehensive portal to the agents for managing total insurance business with OICL through one window.		
1.7.1	Edit profile	The agents are able to edit the information.		
1.7.2	Change password	The Agents are able to change their password if they want		
1.7.3	Buy a new policy online	The Agent can buy all the new products specified in section 3		
1.7.4	Renew the existing policy of OICL	The Agent can renew all the policies specified in section 4 of OICL		
1.7.5	Renew the existing policies of companies other than OICL	The Agent can renew the motor policy from the companies other than OICL		
1.7.6	View saved proposals	The Agents are able to view the saved proposals related to policies.		
1.7.7	View communications	The Agent can view or make a communication in the portal to the desired agent group		
1.7.8	Agency Commission	Commission details for all the policies sold by the agent from portal and also from INLIAS office. Details are fetched from INLIAS.		
1.7.9	Discussion Forum	The Portal allows logged in Agent for participating in a Discussion Forum. The Agent can view or make discussions		
1.7.10	Search Policies	View/search of all policies underwritten by the Agent can be shown on request.		
		Details are fetched from INLIAS.		
1.7.11	Search Claims	View/search of Status/details of all claims intimated for the policies procured by the agents.		
		Details are fetched from INLIAS.		
1.7.12	E forms	The Agent can download the e forms for all the policies and he can view details of all submitted e forms and he can also able to generate the unique key for uploading the e forms.		
1.7.13	Agent Documents	It contains all the Agent documents.		
1.7.14	Download Policy	Agents should be allowed to download policy in PDF format from the Portal		
1.8	Brokers Portal	Comprehensive portal to the Brokers for managing total insurance business with OICL through one window.		
1.8.1	Edit profile	The Brokers are able to edit the information.		
1.8.2	Change password	The Brokers are able to change their password if they want		
1.8.3	Home	The Brokers home page contains the number of documents issued in the current month, during the financial year upto last month, premium collected in the current month, total premium collected during the financial year upto last month, brokerage earned in the current month, total brokerage earned during the financial year up to last month and the broker also gets the alerts.		
1.8.4	Buy a new policy online	The Broker can buy all the new products specified in section 3		

1.8.5	Renew the existing policy of OICL	The Broker can renew all the policies specified in section 4 of OICL		
1.8.6	Renew the existing policies of companies other than OICL	The Broker can renew the motor policy from the companies other than OICL		
1.8.7	View saved proposals	The Brokers are able to view the saved proposals related to policies.		
1.8.8	Search Policies	View/search of Details of all policies underwritten by the brokers is shown on request of the logged in Broker.		
		Details are fetched from INLIAS.		
1.8.9	Search Claims	View/search of Status/details of all claims intimated for the policies issued through the brokers.		
		Details have to be fetched from INLIAS system and Detailed Specification would be decided at SRS phase.		
1.8.10	Claims	Broker is able to intimate a claim behalf of his customer policy with required details. Once a claim successfully accepted by portal the details are sent to INLIAS database for updation and claim intimation number generation.		
		This may trigger an alert to the Office concerned/service center/customer. The broker can also view his already intimated claims.		
1.8.11	Check Renewals	On request by the broker, only View of renewal due of policies procured by the brokers can be shown on Portal.		
		Details are fetched from INLIAS.		
1.8.12	View communications	The Broker can view or make a communication in the portal		
1.8.13	Discussion Forum	The Portal allows logged in Broker for participating in a Discussion Forum. The Broker can view or make discussions		
1.9	Dealers Portal	Comprehensive portal to the Dealers for managing total insurance business with OICL through one window.		
1.9.1	Edit profile	The Dealers are able to edit the information.		
1.9.2	Change password	The Dealers are able to change their password if they want		
1.9.3	Home	The dealers home page contains the number of documents issued in the current month, during the financial year upto last month, premium collected in the current month and total premium collected during the financial year upto last month.		
1.9.4	Buy a new policy online	The Dealer can buy a new policy for Motor insurance only		
1.9.5	Renew existing policy from OICL	The Dealer is able to renew only Motor insurance policy from OICL		
1.9.6	Renew existing policy other than OICL	The Dealer is able to renew only Motor insurance policy from other than OICL		
1.9.7	View saved proposals	The dealers are able to view the saved proposals related to Motor insurance		
1.9.8	Policies	View/search of Details of all policies underwritten by the Dealers is shown on request of the logged in Dealer.		
		Details are fetched from INLIAS.		
1.9.9	Claims	View/search of Status/details of all claims intimated for the policies issued through the dealer.		

		Details are fetched from INLIAS..		
1.9.10	Check Renewals	On request by the dealer, only View of renewal due of policies procured by the dealers can be shown on Portal.		
		Details are fetched from INLIAS.		
1.9.11	View communications	The dealer can view or make a communication in the portal		
1.9.12	Discussion Forum	The Portal allows logged in dealer for participating in a Discussion Forum. The dealer can view or make discussions		
1.9.13	Bulk Upload of proposal data (Motor) in specified format for issuance of policy and processing.	Uploading facility for batch policy for limited number of data in a specified format.		
		The file in a specific format is allowed from the specific dealer and from Portal the file is sent to INLIAS for processing.		
		Portal acts as an intermediate media in this case. The dealer can able to create bulk policies, Open declaration generation and risk uploading and he can download the document templates.		
1.10	TPA Portal	This portal is for all OICL’s tied up TPAs.		
1.10.1	Edit profile	The TPAs are able to edit the information.		
1.10.2	Change password	The TPA can change their password if they want		
1.10.3	View premium	The TPA is able to view premium details		
1.10.4	Search Service charges	The TPA can able to search for details of Service charges.		
1.10.5	policy details	Policies details corresponding to the TPA are available for the TPA. Policy details are fetched from INLIAS on TPA request.		
1.10.6	View communications	The TPA can view or make a communication in the portal		
1.11	Surveyor Portal	This portal is for all OICL’s tied up Surveyors.		
1.11.1	Edit profile	The Surveyors are able to edit the information.		
1.11.2	Change password	The Surveyors are able to change their password if they want		
1.11.3	fees paid	The Surveyors able to view fees paid details		
1.11.4	My pending tasks	The surveyor is able to find his pending tasks.		
1.11.5	view completed tasks	The surveyor is able to find his completed tasks.		
1.11.6	alerts	The surveyor is able to view the alerts and send the alerts.		
1.12	Advocate Portal	This portal is for all OICL’s tied up Advocates.		
1.12.1	Edit profile	The Advocates are able to edit the information.		
1.12.2	Change password	The Advocates are able to change their password if they want		
1.12.3	fees paid	The Advocates are able to view fees paid details		
1.12.4	My pending tasks	The Advocate is able to find his pending tasks.		
1.12.5	view completed tasks	The Advocate is able to find his completed tasks.		
1.12.6	alerts	The Advocate is able to view the alerts and send the alerts.		
1.13	Pensioner Portal	This portal is for all pensioners of OICL company		
1.13.1	Change password	The pensioners are able to change their password if they want		
1.13.2	Pensioners corner	The pensioners are able to view all the circulars related to them.		
1.14	Employee Portal	Employees of OICL are able to access the portal to view and download information.		
1.14.1	Edit profile	The employees of OICL are able to edit the changes of their profile		
1.14.2	Change password	The employees are able to change their password if they want		

1.14.3	Employee Search	The portal allows to search the employees of OICL based on Employee code, Employee Name, Designation, Office Name, Office Code etc.		
1.14.4	Employee Corner	The Employees are able to view & download of Circulars, Notices, PDF, Zip and news articles		
1.14.5	Discussion Forum	The Portal allows logged in employee for participating in the Discussion Forum.		
1.14.6	Grievances	The employees are also able to Register and search the Grievances		
1.14.7	Intimated claims	The employees are able to search the intimated claims		
1.14.8	Proposals	The employees are able to search the Proposals		
1.14.9	Tasks	The employee can view his pending tasks, assigns tasks to other employees, view his tasks and he can view his closed tasks.		
1.15	Portal Admin	View Portal Related Information's		
1.15.1	**Dashboards**			
1.15.1.1	Agent	It contains the information of number of policies issued, Premium collected, commission earned by the agent in current month, during the financial year upto last month and licence expiry date of the agent		
1.15.1.2	Broker	It contains the information of number of policies issued, Premium collected, commission earned by the broker in current month, during the financial year upto last month and licence expiry date of the broker		
1.15.1.3	Dealer	It contains the information of number of policies issued, Premium collected, by the dealer in current month, during financial year upto last month and CD Balance		
1.15.1.4	Surveyor	It contains details of the tasks assigned to surveyor like Task Name, Task assigned by, last date and Policy number		
1.15.1.5	TPA	It Contains Premium and service charges office wise, Month wise and Year wise of the TPA		
1.15.1.6	Advocate	It contains details of the tasks assigned to advocate like Task Name, Task assigned by, last date and Policy number		
1.15.2	**Portal related Information**			
1.15.2.1	Clicks on portal	The number of hits on the portal can be viewed based on the dates		
1.15.2.2	Registrations	Number of Registrations of the customers, Agents, Brokers, Dealers, TPAs, Surveyors and Advocates based on the from date, to date and office code.		
1.15.2.3	Policies issued / premium collected through portal	It contains the reports related to number of policies issued and total premium collected through portal based on dates, office code, user type, user id, policy number, type of policy		
1.15.2.4	Claim Intimation	It contains the reports related to number of claims intimated based on date wise, office code and userid.		
1.15.2.5	Marine Declarations	It contains the reports related to number of Marine Declarations based on date wise, Policy no. and userid.		

1.15.2.6	Proposals	Using this option the user can search for the policy based on the proposal number		
1.15.2.7	User Validations	It shows details of the user(valid or not) based on user type and userid		
1.15.3	**Download Documents**			
1.15.3.1	Download Policy Documents	It allows to download the policy documents		
1.15.3.2	Marketing Office reports	It shows the Marketing reports on the parameters of Month and year		
1.15.4	**Manage Data**	It contains the OICL offices, Employees and Corporate customers		
1.15.4.1	Manage Offices	It contains the information of all the OICL Offices. The portal allows to view the office details, update the office details, create a new office, Downloading of office details and office, city audit trails.		
1.15.4.2	Manage Employees	It contains the information of all the OICL Employees. The portal allows to view the employee details, Update the employee details create a new employee and audit trails.		
1.15.4.3	Manage corporate customers	The portal allows to add a corporate customer, register of policies to corporate customers and audit trails.		
1.15.5	**Manage users/Manage portal**	The portal allows to manage the all users.		
1.15.5.1	Manage Agent Registrations	The portal allows to view and update the details of the agent.		
1.15.5.2	Mobile Shortcode Details	It contains the information of the mobile shortcode details.		
1.15.6	Manage Grievances	It consists of 1. Search grievances. 2. View Grievances. 3. Generate grievance reports. 4. Generate Grievance Receipts. 5. View Pending transfer Grievance requests 6. Upload IGMS Grievance reports 7. Download IGMS Grievance reports 8. View Audit trail		
1.15.7	Payment reconciliation	The admin can reconcile the payments. He can search payment reconciliation, process payment reconciliation and intimate payment reversal		
1.15.8	**Ability to do user profiling**	Super Admin user can provide roles and access to the Admin Users		
1.16	Grievance Redressal	The grievance redressal functionality involves a maximum of 4-level workflow, which is built into the portal application.		
1.16.1	Register Grievance	The Portal allows the users to register a grievance.		
		Grievance details like nature of grievance, cause of grievance and office, etc. is captured.		
		Only policyholder of Oriental can register a grievance on the portal.		
		On successful grievance registration the portal allows the user to take printouts as acknowledgement with complain number in it.		
		On registration an alert Email is generated from the system to different level (operating office, DO, RO and HO).		
1.16.2	Update status/reply of Grievance	Customer Service department of OICL from BO, DO, RO and HO are allowed a login to reply to the grievance and update status of such grievance.		
1.16.3	Status of Grievance	The status of the grievances can be retrieved from the system and is shown to the Complainant.		

1.16.4	Complaint register	View Reports like pending and closed cases for group of users based on a particular role and privilege.		
1.16.5	Report on pending cases with different level	View Reports like pending and closed cases for group of users based on a particular role and privilege.		
1.16.6	Grievance analytical reports.	View Analytical Reports like Case Age-wise, Cause wise, and Nature of grievance wise Reports.		
1.17	SMS and email alerts for Policyholders	The portal has interface with SMS gateway and email server thereby enabling messages and alerts to be sent to customers.		
1.17.1	Alerts to customer and businesses partners about policy issuance confirmation, claims tracking information, and additional benefits.	The registered customers/policyholders/other users get SMS and email alerts on Confirmation of online transactions.		
1.17.2	Alerts to events on portal (e.g. newsletter releases, events).	SMS and email alerts for specific activities should also be sent to internal users.		
1.17.3	The INLIAS also provide some trigger for internal/external SMS/email trigger to happen from Portal			
1.18	Common website Contents	All the contents of existing web site is shifted with latest modifications, to the portal.		
1.18.1	**About Us**	It provides the information regarding Company profile, Objectives, Vision, Mission and Management structure.		
1.18.2	**Products**	Products and Offerings consists of all the products which are offered by OICL. It contains the product description, policy wordings, Terms and conditions and Exclusions		
		Motor - Two wheelar package policy, Private Car Package policy, Commercial vehicle package policy, Liability only policies(Applicable for all types of vehicles), Motor trade Policies, Motor Trade Internal Risk		
		Health - Individual Mediclaim		
		Personal Accidents - Individual Personal Accident Policy, Janata Personal Accident Policy		
		Travel - Overseas Mediclaim Policy		
		Shop Keepers - shopkeepers policy		
		Home - Householders Insurance Policy, Sweet Home Policy		
		Happy Family - Happy Family Floater Policy		
		Nagarik Surksha - Nagarik Suraksha Policy		
		Marine - Marine Master Declaration Policy		
		Premium calculators for all the New policies to be purchased from portal are available for all portal visitors. This calculator is available for Individual Mediclaim, Happy family floater policy,		

1.18.3	Premium Calculators	Personal Accident Policy, Janata Personal Accident Policy, Overseas Mediclaim Policy, Package policy for Private Car and Motor Cycle, Shop Keepers Policy,		
		Householders Insurance Policy and Nagarik Suraksha Policy.		
1.18.4	Download Policy Document	The Customers can Download the Policy Document from our Web Portal using Policy Number, Insured Code and Expiry Date.		
1.18.5	Contact us	It Shows the Contact Address, Email ID's and Contact Numbers of the Registered office		
1.18.6	FAQ	It provides brief information about frequently asked Questions.		
1.18.7	**Office Locator**	The System has the ability to locate our Offices and Contact Points with the help of Office Locator and Visual map.		
1.18.7.1	Locations of OICL Offices	If the user clicks on this option, it is shown the map which contains all the regional offices. If the user clicks on any of the regional office on the map, it is shown list of all the offices under that Region.		
1.18.7.2	Foreign offices	In this section, the user can view the list of all the foreign offices of the company.		
1.18.8	News Alerts	it provides latest news, articles related to Our company, General Insurance etc.		
1.18.9	**Oriental insurance**			
1.18.9.1	Management	It provides the information regarding Company's Management structure and Profile information		
1.18.9.2	Senior Executives	It provides the information regarding Company's Senior Executives.		
1.18.9.3	Citizen's charter	It contains the details of the Citizen charter		
1.18.9.4	Annual Reports	It contains annual reports and financials of the company		
1.18.9.5	public disclosures	It contains all the NL forms of the financial year		
1.18.9.6	Performance	It contains financials of the company		
1.18.10	**Customer Services**			
1.18.10.1	Network Hospitals	It contains the list of Network hospitals and addresses		
1.18.10.2	Disclaimer	It contains the Disclaimer		
1.18.10.3	Refund/Policy Cancellations	It contains the rules for refund or policy cancellations		
1.18.10.4	Claim Documents	It contains claim documents for different types of policies		
1.18.11	**Miscellaneous**			
1.18.11.1	Careers	Careers module contains the information related Recruitments. It consists Advertisements, applications and results.		
1.18.11.2	Tenders	It contains the tender notices of the company		
1.18.11.3	RTI Act	It contains the information related to RTI Act.		
1.18.11.4	Vigilance	It contains the information related to Vigilance.		
1.18.11.5	Business partners	It contains the information related to Business partners like Agents, Brokers , Dealers and etc. and their responsibilities.		
1.18.11.6	Service Providers	It contains the information related to Service providers like TPAs, Surveyors, Advocates and etc. and their responsibilities.		
1.18.11.7	Employees	It contains the information related to Employees/Pensioners of the company and their responsibilities.		

1.18.12	Help	The portal contains the help section which consists step by step procedures to help the users of the portal to work in the portal.		
1.18.13	Tips on Insurance	It provides detailed information about Insurance policies and coverage etc. which is the most suitable policy for a customer.		
1.18.14	Testimonials	It contains testimonials		
1.18.15	Have us call u	It contains the Have us call u section		
1.18.16	**Web Site Usage**			
1.18.16.1	Site Map	it provides list of pages of our web portal accessible users.		
1.18.16.2	Terms and conditions	It contains general terms and conditions		
1.18.16.3	Privacy policy	It contains Rules of Privacy policy		
1.18.16.4	Links	It provides access to some of the important websites such as IRDA, GIC, Insurance Ombudsman, TAC, NIA Pune, III etc.		
1.18.17	OICL Portal integration with CSC Portal.	Integration of OICL portal with the web portal of Common Services Centre (CSC) (www.apna.csc.gov.in) which is a Government of India initiative of the Department of Electronics and Information Technology under the National e-governance plan.		
1.18.18	OICL Portal integration with Web aggregator	Integration with various Web aggregator is required where the portal will receive web service calls from aggregators and send the details to INLIAS for premium calculation and generation of policies. So multiple web service may be developed for this generic module. In future OICL may add or remove any aggregator with minimum effort.		
1.18.19	OICL Portal integration with Broker Portal	Integration with various Broker is required where the portal will receive web service calls from Brokers and send the details to INLIAS for premium calculation and generation of policies. So multiple web service may be developed for this generic module. In future OICL may add or remove any Broker with minimum effort.		
1.18.20	OICL Portal integration with Bank insurance Partners	Integration with various Banks is required where the portal will receive web service calls from Bank branches and send the details to INLIAS for premium calculation and generation of policies. So multiple web service may be developed for this generic module. In future OICL may add or remove any Bank with minimum effort.		
1.18.21.1	Enhancements in access to Motor dealers. Online Policy generation at dealers end thru web service call from dealer system	A generic module has to be developed to accept web service calls from Dealer system and data in specified format allowed to sent to INLIAS for processing and generation of policies.		
1.18.21.2		Portal will act as an intermediate media in this case. The dealer will able to create policies thru web service call and download the policy document from the portal.		
1.18.22	Cash Deposit and/or Web Wallet facility	Cash Deposit and/or Web Wallet facility for dealers / agents / Brokers. Certain selected dealers, agents & Brokers may be given password driven web wallet / cash deposit facility so as to enable them to issue policies without using credit card / Net banking.		

1.18.23	Generation of renewal reference number on portal and through short code SMS.	Premium collection at operating office for a reference number generated on portal without requiring approval of proposal by the operating office. Generation of renewal reference number on portal and through short code SMS. The renewal reference number is already generated in INLIAS and communicated to portal. However this should appear on the first screen in portal. The INLIAS in office should be able to accept this renewal reference number and premium quoted. Similar facility should be available through short code SMS.		
1.18.24	Mobile and Native application	The Bidder is expected to develop the mobile version of the portal. The mobile version of the Portal should compatible with major mobile browsers and display on mobile browser quickly with minimal bandwidth requirements. While offering a simple and clean layout, the website should also implements top security measures such as 256 bit SSL encryption to protect communications.		
		The following services would be provided to the mobile users with mobile native and mobile web application to run on android, windows, iOS, blackberry OS platform		
1.18.24.1		• New Policy purchase		
1.18.24.2		• Renewal Premium on the OICL expiring policy		
1.18.24.3		• Expiry date of the OICL policy		
1.18.24.4		• Renewal of the OICL policy		
1.18.24.5		• Quick Claim Intimation		
1.18.24.6		• Track Motor Claim status		
1.18.24.7		• List of network hospitals		
1.18.24.8		• Locate nearest OICL office		
1.18.24.9		• Agent Locator		
1.18.24.10		• Feedback of customers		
1.18.24.11		• Messaging Service includes - Enquiry using SMS,USSD.		
1.18.25	Document Upload	Document upload should be available on the portal against document checklist as per the product.		
1.18.25.1		This feature should be customizable.		
1.18.25.2		The document upload status should be updated back in INLIAS		
1.18.25.3		Automatic mailing of uploaded document to the designated recipient.		
1.18.26	Policy search & downloads	Enabling policy search through registered Mobile number.		
1.18.26.1		The bidder is expected to implement search engine optimization with the following:		
1.18.26.2		Search Engine Indexing – submit our portal to Google, Yahoo!, Ask.com, and other popular search engines to ensure we are indexed.		

1.18.27	Search Engine Optimization.	Meta-Tags, Keywords, & Page Titles – ensure that each web page has the appropriate page title, keywords, or any other meta-tags that are required.		
1.18.28.1		Natural Search Optimization – test content structure, linking strategies, and sitemap to ensure consistent natural search engine page rankings. Follow Google's 'PageRank' methodology and Webmaster Guidelines to ensure best practices are followed. OICL expects to be found within the first 10 results.		
1.18.29	Social Media Integration	The Portal should provide for social media integration i.e. Facebook, Twitter and Youtube, and other common social media applications. The Bidder is expected to integrate the proposed Portal with various social media		
1.18.30	Kiosk accessibility	The portal can be accessible from touch-screen kiosks installed at select locations.		
1.18.31	Online Live Chat in Portal	Online Chat facility need to be provided for various stake holders to communicate with a team from OICL.		
1.18.32	Quick quote	Quick quote facility should be available in the portal to get the quote in a faster way. Portal need to communicate with INLIAS for this service on portal.		
1.18.33	E forms	The portal should allow the stakeholders to upload certain E form in their login, which can be downloaded concerned office for official purpose. Following e forms should be designed by the Bidder with required validations.		
1.18.33.1		1. Proposal Form		
1.18.33.2		2. Claim form		
1.18.33.3		3. Discharge Voucher		
1.18.33.4		4. Bank Details		
1.18.34.1	CD Account	Cash Deposit (CD) Balance and status is to be shown for Customers.		
1.18.34.2		Details have to be fetched from INLIAS.		
1.18.35	Automatic Generation of failed transaction log	Mechanism should be developed and implemented by the Bidder for automated generation of failed transaction log		
1.18.36	**Agents**			
1.18.36.1	Renewals query	Renewal notice for a particular policy should be visible to the agent on request		
1.18.36.2		Details are fetched from INLIAS.		
1.18.36.3	New Business Requests	Agents can request for new business through portal where approval is required from office.		
1.18.36.4		On request for new business an Email and SMS alert is sent to the concerned office.		
1.18.36.5	What's New	On agent login the what's new specific for him should be display to the agent.		
1.18.36.6	Different level of access to different category of agents,	Different level of access to different category of agents like CMD club members. Features availability should accordingly allowed.		

1.18.37	**TPA**			
1.18.37.1	Upload facility of claims settlement and Claims Payments for TPAs	Details of claims settlement records need to be sent to INLIAS for updation.		
1.8.37.2	Facility to upload reports, images, audio and video) and attach these to claim record	Upload of reports/files to attach with specific policy/claim.		
1.18.37.3		On upload Email and SMS alerts should be generated from the system to respective operating office.		
1.18.37.4		Detailed Specification would be decided at SRS phase.		
1.18.38	**Dealer**			
1.18.38.1	Issuance of Policy	Issuance of Policy/ Renewals against the CD account		
1.18.38.2	Underwriting Discount	Facility to enter underwriting discount upto the limit defined for the dealer		
1.18.39.3	Upload Proposal	Upload of proposal data in excel format for issuance of policies		
1.18.39.4	CD Balance	Cash Deposit (CD) Balance and status is shown for specific dealers.		
1.18.39.5		Details have to be fetched from INLIAS.		
1.18.39.6	Policy Details	Policy details for a given period for a dealer to be displayed		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
1	Based on Service Oriented Architecture that can interoperate/integrate with other application. Real-time integration with core system (INLIAS) is required.		
2	The proposed portal solution should be compliant to the latest versions of W3C standards on 'Web Design and Applications'.		
3	The Proposed portal has to meet WCAG 2.0 accessibility levels: A, AA & AAA.The portal must be disabled friendly		
4	Supports Security protocols and Digital certificates for secure authentication.		
5	The proposed portal solution should able to use HTTPS as the communication protocol, i.e., HTTP over an encrypted secure socket layer (SSL). The solution should support secure transmission of data over the network and support SSL.		
6	The proposed portal solution including the hardware should comply to IPV6 Protocol.		
7	Rule based Personalization as key feature and native to the Portal Server.		
8	The proposed solution should automatically control access to portal resources using business rules based on user profile, preferences, session, time, or http request attributes defined in user repository which can be database or LDAP v3		
9	The proposed solution should provide access to the content and applications for which the user is qualified		
10	The proposed solution should support multi-tier authentication where required.		
11	The proposed solution should Provide for Security as per CERT-In guidelines		
12	Portal client pages support cross-browser running on different Operating System (Compatibility with different versions of IE, Mozilla, Firefox, etc.).		
13	The proposed solution including database should have a Disaster- Recovery (DR) solution to replicate the changes happening.		
14	The proposed solution should support Bilingual (English & Hindi) features for the portal		
15	Portal supports other Indian Language – Please Specify other Languages		
16	The proposed solution to have Dynamic Content Management System (CMS) Features.		
17	The proposed solution should have common document management features like storage, archiving, Check-in/checkout, versioning, and document reviewing.		
18	Web Content management features such as content lifecycle management campaign management, version control, and separation of content items with presentation template so line of business user can manage content with content ownership as key feature and native to the Portal Server.		
19	Content Aggregation from multiple sources such as web content management, enterprise content management, databases, business applications as key feature and native to the Portal Server.		
20	Search And Index contents on web portal, enterprise content sources such as content management, databases, file systems, mail messaging repository etc. where access can be based on role as key feature and integrated to the Portal Server.		
21	Supports and possess Single Sign-On capabilities to aggregate other applications screens onto one page.		
22	The proposed solution (web server, portal application server, Database Server) should provide for Clustering, Load Balancing, High availability/ Fail Over vertically and horizontally.		
23	Application Server should be fully standards compliant providing support for Web Services, SOAP, WSDL, UDDI, LDAP v3, SSL v3, Java 1.3 and XML 1.0 standards.		
24	Availability of Integration layer as a independent service component is available for SOA based integration with different backend systems.		
25	Capable of business process based orchestration and should support straight through as well as long running business processes based on web services etc.		
26	Capability to integrate with the online payment gateway system for All types of online payment system (VISA/MasterCard).		
27	Supports integration with the SMS (Short Messaging Service) to send SMSs programmable on events.		
28	The Portal platform is capable of handling 40000 active users on Portal web server and scalable to 80000 active users within the box.		
29	The Portal should be scalable horizontally for further upgradation in future.		
30	The proposed solution should extend portal coverage to wireless devices, smart phones with web browser and device detection		
31	The portal can be accessible from touch-screen kiosks installed at select locations.		
32	Collaboration such as Discussion Forum as key feature and native to the Portal Server.		
33	The proposed solution to have ability for social media integration i.e. Facebook, Twitter and Youtube, and other common social media applications.		
34	Web Analytics Integration – integrate new website/CMS with existing Google web analytics systems to provide accurate reporting on website activity. The Bidder may choose to use other web analytics so long as the objective is not lost.		
35	The proposed solution should provide Search Engine Optimization, Search Engine Indexing, Natural Search Optimization .		
36	The proposed solution should allow to Measure and understand end user experience in terms of Response time and Availability Tracking Portal Usage		
37	Provides Audit trails, auditing of user actions and document history		
38	The proposed solution to have Archives Management.		

39	**Web Content Management System**
39.1	**Content Management and editing**
39.2	The Portal application shall provide the following content management requirement;
39.3	easy content editing, shall be as easy as editing in Microsoft Word. Menu links shall be automatically generated as editors add/delete pages.
39.4	the facility to define Content Authoring Templates which can allow business users to author content
39.5	Menus and sub-menus shall be dynamic and created, based on the page-tree as pages are added and subtracted. The webpages shall be styled entirely through CSS (Cascading Style Sheets), with clear and appropriate graphs. Once the authorized user makes any changes, the system shall be able to record those changes including time, date, user details and section of the site modified.
39.6	Bilingual content(English and Hindi) shall be managed from the same control panel. Add/Edit/Delete of content for both languages from the same page should be allowed.
39.7	Allow inserting metadata for each page globally and for different languages
39.8	Should support managing all content using a workflow from creating content to publishing content. Which shall help to test & plan website upgrade easily & effectively.
40	**Portal Applications and Page Management**
40.1	The Portal application shall provide the following Portal Applications and Page Management requirement;
40.2	Modular UI Theme support for improved web page performance
40.3	Provide support for independently configured logical portals (virtual) on same physical portal
40.4	Must support responsive web design and multi-channel rendering of applications and content on smart phones, tablets, desktops and kiosks without duplicating the application code or logic.
40.5	Ability to reuse portlet instances on several pages of portal
40.6	Ability to persist user's session, including current location in portal, across browser sessions
40.7	Support configurable user friendly relative URLs for direct access to pages
40.8	Support declarative inter-portlet communication/messaging
41	**Scheduling**
41.1	The Portal application shall;
41.2	allow content to be published and unpublished on specified dates.
41.3	allow version control of content & ability to rollback
41.4	Allows site based creation and publishing of content
42	**Social Media Integration**
42.1	The Portal application shall integrate with social media such as Facebook, LinkedIn, Twitter, Google+ and YouTube. This shall also include the ability to "Like", "Share", "Print" and "E-mail" this page.
42.2	Should provide integration with social channels to PUBLISH your approved web content items on social networks.
42.3	Blogs - The Portal application shall provide a platform to display industry and site blogs.
44	**Marquee**
44.1	The Portal application shall support configuring a scrolling marquee. The marquee speed, direction and behaviour should be configurable.
45	**Mashups**
45.1	The Portal application shall support setting up of mashups that can then be displayed on the site/portal.
46	**Multilingual**
46.1	The Portal application shall allow the sites/portal to be configured in languages identified by the Constitution of India.
47	**Workflow**
47.1	The Portal application shall allow creating workflows that can be associated with content.
47.2	The Portal application shall provide a trigger facility to send a reminder notifying about the expiry date of the content and once the notification is sent, it shall be ensured that either the content is placed in the archive section or the expiry date is extended.
47.3	The Portal application shall provide reusable process workflows
47.4	The workflow should be coupled to the code (Tightly coupled / Medium coupled / Extremely configurable) *Please specify the extent to which it has been coupled.*
47.5	Ability to program the workflow actions
48	**Content Integration**
48.1	Content hierarchy and meta-data shall be available via RSS Feed to other content management systems
48.2	The Portal application shall provide Integrator component which defines standard based interfaces to consume content from other custom made systems – Making it easy to ingest content from external systems

49	**Document Viewer**
49.1	The Portal application shall provide content components like document viewer /catalogue to be available that helps in previewing content without downloading content
50	**Document Management System**
50.1	**Central Document Repository**
50.2	A central document repository shall be applied on many levels (user level, department level, institution level), and these repositories will contain all the shared files according to its level, this requirement must be applied using a Document Centre Site.
50.3	Document Repository should have an interface to access content from repository that will support upload, rating, workflow etc.
51	**Document Upload**
51.1	Every user will have the ability to upload any number of file depending on the storage available on the server not according to a specific number of files, therefore the files count should be unlimited.
51.2	The Portal application shall allow bulk upload of documents.
52	**Workflow**
52.1	The Portal application shall allow configuring workflow for the documents. The workflow can be manual where user decides whom to send it to, and Rule based workflows where the administrator creates a rule to dictate the flow of the document.
53	**Archiving**
53.1	All the documents and files created from this solution and the workflows must be archived for later use. All the files that will be archived should have pre-defined parameters for both In-Coming and Out-Going correspondence.
54	**Document Sets & Content Types**
54.1	Creation of document sets is essential to insure integrity and consistency.
55	**Versioning & Collaboration**
55.1	The Portal application must have the ability to create a version of the document each time it has been edited or changed through Check-In\Check-Out technique and content approval before document publishing, and many users should have the ability to work on the same file using the pre-mentioned techniques.
56	**Information Rights Management**
56.1	All IRM features must be enabled to protect documents and files on all levels
57	**Microsites/ Sub Sites**
57.1	The Portal application shall allow setting up of microsites/sub sites.
58	**Moderation**
58.1	The Portal application shall provide a way to moderate the user generated comments, ratings, reviews.
58.2	The Portal application shall have the ability to define lists of keywords which should be blocked or allowed
59	**Segmentation & Targeting**
59.1	Portal must support English based rules engine for segmentation and targeting
59.2	Portal must support recommendations (alternate product suggestions)
59.3	Portal must support anonymous user segmentation
60	**Architectural & Design Aspects**
60.1	The Portal application shall be compliant to the latest versions of W3C standards on 'Web Design and Applications' standards available at http://www.w3.org/standards/webdesign/
60.2	Support for tight integration with WS - JAXRPC, JAXWS (Web Services std) & JAXRS
60.3	AJAX based JSF components - for rich UI ,web 2.0 components
60.4	The Portal application shall support multi- tier architecture for all modules within The Portal application with well defined interfaces between the layers
60.5	The Portal application shall have the ability to scale horizontally without redesign
60.6	The Portal application shall support the deployment on multiple similar hardwares and mix of multiple hardwares in a horizontal setup.
60.7	The Portal application shall have the ability to scale vertically without redesign
60.8	The Portal application shall support the addition of CPU, Memory, Hard disk capacity without causing downtime
60.9	The portal application shall be designed for ease of maintenance and readily allow future functional enhancements. This shall be accomplished through use of modern design principles like applying principles of modularity, interface abstraction, and loose coupling.
60.10	The Portal application shall have the modular structure providing the flexibility to deploy selected modules-products- lines of business combination as per the Organization's convenience and shall be adequately flexible to keep up with the changing technology.

60.11	The portal application shall be scalable and adaptable to meet future growth and expansion/contraction needs such that the website can be expanded on demand and be able to retain its performance levels when adding additional users, functions, and data.
60.12	The portal application shall provide the ability to create and/or modify edits and business rules which determine the correctness/integrity of data.
60.13	The portal application shall provide the ability to create and/or modify edits and business rules which determine the correctness/integrity of data.
60.14	The Portal application shall support the deployment of additional modules at a later point in time with minimal downtime and loss of productivity.
60.15	The Portal application shall support the following:
60.16	exception handling
60.17	logging,
60.18	security (access control architecture),
60.19	message encryption
60.20	The Portal application shall support message patterns and protocols supported - e.g. publish/subscribe, synchronous/asynchronous, push/pull/pool, topics/queues.
60.21	The Portal application shall support seamless integration of new services into existing structure without significant changes or effort.
60.22	The Portal application shall provide for remote procedure calls and web service calls through standard protocols like RPC, SOAP, CORBA, etc. and should support communication through XML integration.
60.23	There should be configuration management tools (version control) available for the product. Please specify whether the tools are UI or program coded. Please specify the tool if not inbuilt function in the Portal Software.
60.24	All parameterization, configuration, creation of rules and reuse of rule in the product shall be user interface driven
61	**Performance & Interoperability**
61.1	The portal framework architecture should be flexible that exposes integration points at many levels, including presentation, proxy, WSRP(Web Services for Remote Portlets), and fully exposed and supported web services (SOAP), JSON, & RMI.
61.2	The portal application shall have the ability to support replication and failover using high-availability architectural options.
61.3	The portal application shall have the ability to support either a Production and hot (real time replication) disaster recovery design or a multi host site Production design that would allow one site to seamlessly be offline and the other site would maintain service without interruption.
61.4	The portal application shall provide the ability to recover from data loss due to end user error and end application error.
61.5	The portal application shall provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.
61.6	The portal application shall provide tools for managing an environment that supports both high availability and disaster recovery.
61.7	The portal application shall include the capability to maintain all data according to Company defined records retention guidelines (i.e. record schedule).
61.8	The portal application shall include the capability to maintain all images and electronic documents according to Company defined document retention guidelines (i.e. record schedule)
61.9	The portal application shall provide on-line access of the current and previous financial year data for auditing purposes at any point in time.
61.10	Ability of The Portal application to run on the latest version of the operating system:
61.11	The Portal application should interoperate data between applications through standard interfaces with supporting enterprise data model for data integration
62	**Deployment**
62.1	The portal application shall adhere to standards and guidelines that will allow the content to be migrated to an alternate platform with minimal efforts.
62.2	The portal system must have automated deployment scripts for managing applications, pages and other portal artifacts, hence must reduce manual intervention.

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
	Security		
	Authentication		
1	Application should be able to determine if the user is who he/she claims to be.		
2	Common form of ensuring Authentication is user-id and password based authentication. OTP based authentication must also be supported. Any additional software component required to be provided by the bidder.		
3	Secure transmission of account credentials and mission critical data (SSL)		
4	Developing Authentication policies/processes and documenting the same in order to ensure unauthorized users are kept at bay.		
5	USER_ID's should only be used to identify and reference users and not as proof of identity or authentication mechanism.		
6	To prevent a reuse of the same passwords or similar passwords thereby enhancing security, a password history must be maintained. The system must securely memorise the last 3 passwords, and accept only a new password which differs from the 3 previous ones.		
7	An account must be locked after 5 erroneous user authentication attempts and the administrator should be alerted. The account can only be unlocked by the system administrator only upon verifying the authenticity of the user and whether there was no attempt/attack to breach security		
8	A password reset procedure must be defined. The actual password reset may only be done by the system administrator. If in case the reset procedure requires an email to be sent to the user requesting for the change, no usernames/passwords/other sensitive information to be sent in that email. Instead, a link having a certain lifetime should be sent which would prompt a dialogue box for the change		
9	Logging of repeated failed logon attempts		
10	Usage of a common message for authentication errors so as to avoid enumeration attacks. i.e. Never stating/displaying whether the id entered is wrong or the password entered is wrong		
11	Last successful login and the number of failed attempts should be displayed to the users		
12	Change password function should always ask the user for both the old and new password		
13	Authentication and session data should always be submitted as POST		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
14	The application must support the user-id convention as well as password policy as per User Access Policy		
15	Removal of default user accounts (if any)		
16	Implementing CAPTCHA or similar anti-automation security control to avoid DOS, dictionary attacks and brute forcing		
17	Passwords & Secret answers for password retrieval should be encrypted and never be stored in clear text		
	Authorization, Access Control and Role Based Access Control		
18	Application should be able to determine what should the authenticated user be allowed to view		
19	Access control checks to access protected URL must not be by passable by a user that simply skips over the page with the security check.		
20	Application should have a provision of defining roles based on which access would be given		
21	Protection of sensitive links/landing pages		
22	Creating/Defining roles for all the users of the application		
23	Access to various applications integrated with the Portal to be given only basis the defined roles		
24	Administrator panel/ protected URLs to be made available only to authorized users		
25	Disabling directory listing on application servers		
26	Sensitive links which should not be indexed by search engines should be included in robots.txt file.		
	Session Management		
27	Application should be able to protect account credentials and session tokens		
28	Ability to provide unique session ids (Generated randomly by secure random number generators) to authenticated users		
29	Session ids should be protected with SSL		
30	Connection timeout provision		
31	After each reauthenticaiton a new session id should be provided to the user and the previous id should be invalidated. After user logout the session id will be invalidated as well		
32	The domain and path for cookies containing authenticated session identifiers should be set to an appropriately restricted value for the site.(Inserted as is from OWASP)		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
33	Logout links should be available from all pages of the application		
34	After successful authentication operations, users should be redirected via HTTP 302 to internal pages.(Inserted as is from OWASP)		
35	httponly attribute should be set on cookies. In addition, secure attribute should be set on cookies for HTTPS communications.(Inserted as is from OWASP)		
	Data Input & Validation		
36	Validation of all data being entered into the application		
39	Ability to constrain input as per requirements (Manually create input rules)		
39.1	Application input data from HTTP requests must be checked against a defined format which would specify the exact nature of input that should be permitted		
39.2	Server side input checks to be performed. In order to enhance user experience, client side checking should be considered		
39.3	Follow the process of white-listing instead of black-listing		
39.4	There should not be any provision of modifying raw data in the underlying database		
39.5	The application should ensure that pages containing sensitive information should not be allowed to be cached		
39.6	Protection against injection flaws		
39.7	Perform boundary checks of input data		
39.8	Perform data sanitization checks		
40	Any file being uploaded onto the application should be checked for any anomaly in Name, length, type and content of the file		
40.1	**Encryption**		
40.2	Application should be able to encrypt mission critical data		
40.3	Use of cryptographic controls		
40.4	Only using secure algorithms for secure communication over SSL		
40.5	Only permitting strong and complex passwords for administrators		
40.6	**Error Handling**		
40.7	Effective protocols for handling application errors. Ensuring that unnecessary internal details are not displayed to the user when the error occurs		
40.8	Ability to log errors and flag to administrators		
41	Application should never return any system generated messages or other debug information in any of its responses to the user accessing it		
41.1	**Logging**		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
41.2	Application should have the provision of logging all authentication & authorization events		
41.3	Application should have the provision of logging all administrator activity		
41.4	Application should have the provision of monitoring any changes to inbuilt rules/data		
42	Application should have the provision of logging all key transactions taking place through it		
42.1	Application should have the provision of storing logs in a secure manner		
42.2	Logs to be maintained for an agreed pre-defined period		
42.3	**Others**		
44	Regular patching of application frameworks, application servers, database and web servers		
44.1	Enabling all security features of application frameworks		
45	Ensuring that when application is transferred from a development environment into a production (live) environment, all demos, test codes , etc. should be excluded. Comments should be removed from source files		
45.1	The vendor will be able to provide an independent test report stating the application is free from known security defects.		
46	The proposed solution will provide the ability to provide a secure environment that can detect and block common security vulnerabilities such as those identified by the OWASP.		
46.1	Vendor should provide a Vulnerability Assessment-Penetration Testing report for the application before go live		
47	**Usability and Accessibility**		
47.1	The SI shall provide a system user interface that is easy to read, and user-friendly.		
47.2	The system user interface and any system to user communications shall be localized into multiple languages.		
47.3	The user interface shall display text in the end user’s preferred language (if the preferred language is one of the languages listed above).		
47.4	The system should provide a tutorial feature that provides tips for using the website.		
47.5	The system should provide Navigation tabs to allow user to navigate backward through the data and review what was entered, without losing the previously entered data.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
48	The system shall provide summaries at several points allowing applicant to review what has been entered to date and revise that information as necessary, prior to finalizing the data submission process.		
48.1	The system shall provide a mechanism for displaying confidentiality statements and privacy protections wherever appropriate .		
48.2	The system shall provide a mechanism for tracking acknowledgement of documents submitted offline by posts.		
49	The system shall provide a method to access the system by mobile device.		
49.1	The system shall provide a method for the customer to view, print, forward electronically their own service request information.		
50	The SI shall provide web-based access that is fully functional regardless of browser or device		
50.1	The contractor shall provide for resizing of windows to accommodate different monitor sizes and resolution without truncating the windows in the user interface.		
50.2	The SI shall support a single point of sign-on for all activities within the system and ancillary components including but not limited to rules engine, workflow software, web portal, testing tools, data imaging software, and reporting repository. Entry to the web portal shall support single sign-on from an outside secure web portal.		
50.3	**Environments**		
51	The system should be able to support the environments listed below:		
51.1	1. Production		
51.2	2. Test		
52	3. Development		
52.1	4. Migration		
53	5. Training		
53.1	6. Disaster Recovery		
54	The system shall have the tools to replicate, initialize, or populate the environments.		
54.1	All software products that are part of the proposed solution shall be licensed to operate in the development, test, training, UAT, emergency fix and production environments.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
55	The system shall include a system integration test environment that mirrors the production environment in server and application configuration, including but not limited to server and application clustering, load balancing, and deployment strategies used or planned for production.		
55.1	The system shall provide a training environment that enables the ability to easily reset the training data after a completed class or scenario, in order to continue executing multiple training scenarios.		
56	The system shall provide testing environments that integrate with legacy test environments in order to execute data synchronization, conversion, and performance testing conditions that require access to or impact legacy systems as part of the test execution.		
56.1	The system shall provide the ability to perform temporal testing within all non-production environments.		
57	The system shall provide the ability to easily manipulate the system date by a tester for temporal testing		
57.1	The system shall provide a process for extracting all or a subset of data from the production environment and importing into non-production environments for executing test scenarios or troubleshooting production issues with production-relevant data.		
58	The system should provide a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data when extracting data from the production environment for use in non-production environments.		
58.1	**Tools and Performance Monitoring**		
58.2	The system shall provide application management and monitoring capabilities to record metrics including, but not limited to, application health and availability, application uptime, frequency of access for application resources, and resource utilization by application resources.		
59	The system shall provide systems and server level monitoring capabilities to record metrics including, but not limited to, server health and availability, server uptime, and server resource utilization.		
59.1	The system shall be designed with the capability to consistently collect and report metrics from application-level processes in a consistent manner across the application and architecture to support all application monitoring requirements.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
59.2	The system shall provide the ability to configure alerts, including but not limited to, alert thresholds, alert notification channels, and ability to turn alerts on or off for all system and application monitoring capabilities.		
59.3	The system shall provide logging capabilities that promote standardized logging across environments and applications.		
60	The system shall provide the ability to to diagnose errors and to write trace information.		
60.1	The ability to instrument the system's application code shall be configurable at runtime, and should not require explicit intervention of support staff to write and incorporate logic at each point where instrumentation is required.		
60.2	The system shall provide mechanisms to assure a managed level of system integrity through proactive identification of system event patterns or event inconsistencies and issuing alerts to the appropriate incident and problem management processes.		
60.3	The system shall provide management tools for any proposed third party off-the-shelf component, including detailed information regarding contractor, product, and version.		
60.4	**Backup & Restore**		
60.5	The system must provide the ability to perform backups and recoveries of the system including, but not limited to, the database, core and customized software, software and database configuration options, and user preferences and rights.		
60.6	The system must provide the ability to perform backups and restores in a full, incremental and differential manner.		
60.7	The system must support the ability to perform online backups without interruption to system functions or features.		
60.8	**Batch**		
60.9	The system shall include a batch processing architecture in support of batch and asynchronous processing.		
60.10	The system's batch process execution shall provide the ability to leverage the same services and application components as online processes where possible and feasible.		
60.11	The system's batch process execution should not require the online transactional system to be offline during processing.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
60.12	The system's batch process execution shall be capable of being managed by and reporting execution status with job scheduling software.		
60.13	The system shall include a batch architecture that supports event-based batch execution (including on-demand requests) and predefined scheduled execution.		
60.14	The system shall allow administrators to configure batch job sequencing based on outcome of preceding jobs (i.e. job dependencies.).		
60.15	The batch architecture shall provide capabilities for restart and recovery procedures at multiple execution points for failed batch jobs. Each job should provide operational staff the ability to restart, resume, recover, bypass, or cancel, where appropriate.		
60.16	The batch processing solution shall include processing statistics that include, but are not limited to, batch execution time, duration, and execution counts.		
60.17	The batch processing solution shall include appropriate reporting of failures, error conditions, or unexpected terminations, and leverage common error handling and notification routines where possible.		
60.18	The batch solution shall provide the ability to maintain current and historical batch execution reports for operational staff.		
60.19	The SI's solution shall provide a robust extract, transform, and load capability for loading disparate data sources into an analytic database (data warehouse).		
60.20	This batch feed (XI) shall be updated over time as new types of data get added to the Operational Database.		
60.21	**Analytics and Reporting**		
60.22	The system shall include an architecturally distinct, reusable reporting service that facilitates various types of reports, including but not limited to:		
60.23	Static (canned) reports;		
60.24	Dynamic (parameter-driven) reports;		
61	Ad-Hoc reports.		
61.1	The system shall support initiation of reports through various methods, including but not limited to: on-demand requests, scheduled requests, and event-driven requests.		
61.2	The system shall provide ad-hoc reporting capabilities that support drill-down and drill-up functionality.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
61.3	The system shall provide ad-hoc reporting capabilities that enable privileged end users to create reports using defined, user-friendly metadata elements.		
61.4	The system shall provide ad-hoc reporting capabilities that leverage pre-defined relationships and table joins to minimize the risk of executing poorly performing ad-hoc queries.		
61.5	The system shall provide configurable query governance limits for ad-hoc reports to prevent run-away reports from consuming valuable system resources that may impact other system operations.		
61.6	The system shall provide reporting capabilities that do not negatively impact performance on the transactional database.		
61.7	The system shall enforce role-based access control to reports, including but not limited to: 1) Job function or role; 2) Organization, department, and/or region; 3) Report type (operational, business, federally mandated); and Public reports.		
61.8	The system shall generate management reports for monitoring and evaluating office/unit and program performance.		
61.9	The system shall provide the capability to generate operational, transparency and accountability reports.		
61.10	The system shall provide the ability to expose reports through open interfaces, and automatically generate and distribute reports to designated repositories.		
61.11	The SI shall update and maintain all data elements necessary for the reporting.		
62	The system shall include the capability to display summary data in the form of executive dashboards.		
62.1	The Portal application shall provide the analysis like - the popularity of the sites hosted and the visitors' behaviour pattern.		
62.2	The Portal application shall facilitate the view of hits separately for multi-lingual sites/portal. Analysing the visitor hits on the sites/portal should be possible by filtering the data based on certain parameters such as date range, specific page hit. The administrator shall be able to login once to view the number of hits, traffic coming from a specific search engine, keywords used on search engine, repeat and unique visitors and visitor's state and countries. It shall also generate analytics on peak usage time during a particular day/week/month/year.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
63.2	The system shall also provide a facility to generate dashboards of the visitor’s behaviour on a weekly, monthly, quarterly and annual basis. It shall also be capable of generating detailed reports which shall be downloadable in multiple formats. The formats in which the reports shall generate shall be in the formats mentioned below but not limited to these:- .xls .pdf .txt		
	Data Migration:		
64.2	Existing Profiles.		
65.2	Existing transaction details.		
66.2	The descriptive content shall be primarily derived from the existing portal system. The solution should be able to host the content that may be desired on the new portal CMS.		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
	Mobile Device Management Solution		
1	Must support all types of Mobile operating systems		
2	Must support distribution of applications; data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices. This applies to both company-owned and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers		
3	Must support a server component, which sends out the management commands to the mobile devices, and a client component, which runs on the handset and receives and implements the management commands		
4	Must allow a client-initiated update		
5	Must enable the use of an administrative console to update or configure any one handset, group or groups of handsets		
6	Must enable automatic detection of devices in the network and sending them settings for immediate and continued usability. Device Management Centre (DMC) achieves this by filtering IMEI/IMSI pairs		
7	Must maintain history of used devices and send settings only to subscriber devices which were not previously set		
8	Solution must have the functionality to remotely lock and wipe a device, which protects the data stored on the device when it is lost or stolen; and remote troubleshooting		
9	The solution must help provide employees with access to the internal networks using a device of their choice		
10	Must offer secure configuration, file synchronization and sharing capabilities for mobile devices with policy enforcement on document manipulation and application access		
11	Must enable enforcement and support of standard device and data security, authentication, and encryption. Data containerization, application-based-VPN and encryption software are also part of this capability		
12	Must have Network service management ability ie must gain information off of the device that captures location, usage, and cellular and wireless LAN (WLAN) network information, using GPS technology.		
13	Network access control (NAC) features are must also be supported. This is to enforce segmented policies, and can use the network to allow, deny or grant limited access to devices, based on their compliance with these policies.		
15	Must have appropriate firewall and Antivirus capability		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
	Note: Bidders have to ensure 100% Compliance to the below mentioned specifications		
1	Design APIs, gather developers' feedback before implementing		
2	Design from the publishing interface or via importing an existing Swagger 2.0 definition		
3	Deploy a prototyped API, provide early access to APIs, and get early feedback		
4	Mock API implementation using JavaScript or similar convenient scripting language		
5	Supports publishing SOAP, REST, JSON, and XML style services as APIs		
6	TCP/IP adaptors support. Legacy protocols can be supported using custom TCP/IP adaptors		
7	API manager should support custom adaptors based on service standards such as OSGi or similar standards		
8	Supports grouping of multiple APIs based on the version		
9	Publish APIs to external consumers and partners, as well as to internal users		
10	Ability to publish APIs to a selected set of gateways in a multi-gateway instance environment		
11	Support enforcement of corporate policies for actions like subscriptions, application creation, etc. via customizable workflows		
12	Manage API visibility and restrict access to specific partners or customers		
13	Manage API lifecycle from cradle to grave: create, publish, block, deprecate, and retire		
14	Publish production and sandbox keys for APIs to enable easy developer testing		
15	Manage API versions and deployment status by version		
16	Support custom lifecycles		
17	Apply security policies to APIs (authentication, authorization)		
18	Rely on OAuth2 standard for API access (implicit, authorization code, client, SAML)		
19	Restrict API access tokens to domains/Ips		
20	In-built Key Management features - application registration, token generation & token validation		
21	Supports plugging in third-party key servers for application registration, token generation & token validation		
22	Configure Single Sign-On (SSO) using SAML 2.0 for easy integration with existing web apps		
23	Provision API keys		
24	Subscribe to APIs and manage subscriptions on per-application basis		
25	Subscriptions can be at different service tiers based on expected usage levels		
26	Test APIs directly from the web console		
27	View API consumer analytics		
28	Support to act as SSL termination point		
29	Track consumer analytics per API, per API version, per tiers, and per consumer		
30	Monitor SLA compliance		
31	Alerting, real-time dashboards		
32	Publish your own events and create your own dashboards		
33	OOB support for events based on throttling, faults, latency within and from gateway to target		
34	REST API with an extensible security mechanism		
35	Role-based access control for managing users and their authorization levels		
	Governance Features:		

S.No.	Particulars	Bidder' s Compliance (Yes/No)	Bidder's Remarks
36	Access and manage assets via a REST API, supporting the integration with enterprise initiative such as DevOps		
37	Describe relationships between assets such as dependencies, usage or associations and perform impact analysis		
38	Attach custom life cycle to assets and engage custom actions when an asset transitions from one state to the next		
39	Store different type of data or metadata as resources including contracts, models, workflows, WSDLs, Word documents, server configurations and more		
40	Revisions, versions with check pointing and rollback for any resource or resource collections		
41	Customizable dashboards that give users an at-a-glance view as well as details		
42	Real-time alerts (email, sms, push notification, physical sensor alarms, etc.) for instant condition reporting		
43	Expose event tables as an API		
	Expose Data Source as Web Services or REST Resources		
44	- Supported data sources: RDBMS, CSV, Excel, ODS, Cassandra, Google Spreadsheets, RDF, Web page via Odata		
45	- Supported databases: MSSQL, DB2, Oracle, OpenEdge, Teradata, MySQL, PostgreSQL/Enterprise DB, H2, Derby or any database with a JDBC driver		
46	- Supported transports: HTTP, HTTPS, JMS, SMTP, FTP, FTPS, SFTP and TCP		
47	- Support for both JSON and XML media types		
48	- Built-in validators for standard data types		
49	- Customizable validators via Java extensions		

S.No.	Minimum Technical Specification	Bidder's Compliance (Yes/No)	Bidder's Remarks
Note: Bidders have to ensure 100% Compliance to the below mentioned specifications			
	HSM		
1	Support for operating systems like Windows, Linux, Solaris, AIX		
2	Virtual System support for VMware, Hyper-V , Xen, KVM		
3	Host Interface: Should have atleast 4 Gigabit Ethernet ports with port bonding. Should support for 10G fiber network connectivity with port bonding. Should have IPv4 and IPv6 support.		
4	The proposed HSM should come with minimum 5 partitions and each partition should be protected with unique set of userid and password to grant access as per CCA IVG guidelines. The HSM should be able to scale upto 20 partitions on the same box.		
5	Cryptographic APIs: PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL		
6	cryptography: Full Suite B support		
7	Asymmetric: Support for various cryptographic algorithms:Full Suite B support, Asymmetric Key RSA (1024-4096 bits), DSA , ECDSA , ECDH, Ed25519, ECIES, ECC (No separate license of Algorithm to be charged)		
8	Symmetric: AES, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST (No separate license of Algorithm to be charged).		
9	Support for Hash Message Digest HMAC, SHA1, SHA2 (512) and SM3		
10	Key Derivation: SP800-108 Counter Mode		
11	Key Wrapping: SP800-38F		
12	Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG		
13	Digital Encryption: BIP32		
14	5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and Comp128		
15	HSM should be FIPS 140-2 level 3 and CC EAL 4+ certified .		
16	Clustering, Load Balancing should be supported		
17	Ability to generate and Store RSA keys (2048 and 4096)		
18	Keys always remain in FIPS-validated, tamper-evident hardware. Ability to generate and Store RSA keys (2048 and 4096) on board on demand. All Keys must be stored and protected in its FIPS 140-2 level 3 certified cryptographic memory. Minimum 16 GB memory from day one		
19	Multiple roles for strong separation of duties		
20	Secure audit logging		
21	High-assurance delivery with secure transport mode		
22	High quality keys through external Quantum RNG seeding		
23	Securely backup and duplicate keys in hardware with Backup HSM or to the cloud HSM for redundancy, reliability and disaster recovery		
24	HSM should have both Remote and Local multifactor authentication using device and keys for enhanced Security Support.		
25	Safety & Environmental Compliance: FCC, CE, VCCI, C-TICK, KC Mark RoHS2, WEEE, TAA, UL, CSA, CE		

26	Minimum Performance: RSA-2048: 5,000 TPS, ECC P256: 10,000 TPS, AES-GCM: 10,000 TPS		
27	Should Support 170000 Hrs or More		
28	Should be able to integrate with virtual key manager appliance to provide scalability features like Data Discovery & Classification, Transparent Encryption for large scale high performance file system encryption - including specific support for Oracle, Teradata, Pure Storage, HADOOP, SAP HANA and many others		
29	Should Support remote administration for maintaining partitions and adding or removing partitions as business required without the need for accessing HSM physically in DC.		
30	HSM should have the ability to enable / disable policies by HSM commands which will be applicable for Application Users. This feature should not need any Application User login or credentials.		
31	Provide new version upgrades, updates, patches, etc for all the components/ sub-components through the period of contract. 24/7 telephonic and email OEM support through infrastructure based out of India. OEM should be present in India for last 5 years, one PO should be furnished for same. OEM should have their own warehouse in India		
32	The required solution must not be End of Life or End of Support for at least 5 years from the due date of submission of bid by the bidder.		
	KSM		
1	Key Management Platform should be available as both Virtual and Hardware FIPS 140-2 Level 3 form factor directly from OEM. The virtual appliance should support VMware, AWS, Microsoft Azure, OpenStack,Microsoft Hyper-V and Google Cloud Enterprise compatible formats		
2	Key Manager should support Transparent Encryption for large scale high performance file system encryption - including specific support for Oracle, Teradata, Pure Storage, HADOOP, SAP HANA and many others		
3	The System shall support Multi-tenancy using multiple domains, Active-Active Clustering for high availability and Backup		
4	The system shall never transmit sensitive key material over an insecure channel.		
5	The system should support separation-of-duties and policies to be enforced.		
6	Should integrate with users and groups from LDAP, local systems, Hadoop, Teradata and container environments.		
7	Safety Agency Approval FCC, UL		
8	Administrative [interfaces - Secure Web, CLl, SOAP, REST		
9	Network Management - SNMP, NTP, Syslog-TCP.The appliance should support NIC options for 10 GB Fibre		
10	Syslog Formats CEF, LEEF, RFC 5424		
11	API Support -REST, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, NAE-XML , REST, C, Java API's and libraries for integration in to custom applications.		
12	The system shall be capable of managing upto 1,000,000 Keys.		

13	The system should support Built in Data Discovery and Classification with both agent as well as agentless discovery of sensitive PII data using pre-built and customized templates including detection of datatypes within images with OCR feature. It should also include the scanning of local disks , network file shares, big data like hadoop, as well as Cloud storage providers like AWS S3 and Azure Blob.		
14	The Solution should support Intelligent Remediation of discovered sensitive data by encryption .		
15	The Solution should support Custom Infotypes creation using glass for Data discovery and classifcation .		
16	The Solution should support agent based and agent less/proxy scanning of large volumes of data, stored on premise. This includes the scanning of local disks , network file shares and big data like hadoop		
17	The system shall allow KeyCaching, Key rotation and keyVersioning . Key Versioning should not require any downtime for the application.		
18	The system can be configured to send e-mail notifications to specific addresses when system alarms are triggered.		
19	The system should support REST API Tokens (JWT) that are short lived and are used for accessing the REST API for high security needs.		
20	The solution should support vaulted and vaultless tokenization and FPE for Government Identities and PII data.		
21	The system should support active/active clustering of nodes.		
22	Support for Key Management Interoperability Protocol (KMIP) and Database and Linux Key Management to encrypt various data stores like SAN boxes, Tape Libraries, etc.		
23	Should have the functionality of entire Key life-cycle tasks including generation, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets.		
24	The Service Provider shall provide FIPS certified Key archival in accordance with the retention duration stipulated by the customer. The Supplier shall study the user requirements to define the appropriate archival criteria for incorporating and implementing FIPS Certified Key archival and Escrow as part of the solution scope.		
25	The Solution should provide the ability to run scheduled scans to automatically classify files and also have option to pause during peak hours of data traffic .		
26	The Solution should support capability of PDF exporting of Scanned data report .		
27	The KMS should be scalable to key synchronization and Key upload across multiple Public CPS such as AWS, Azure, GCP long with the ability to support automated scheduled key rotation and key expiry via a simple easy to use GUI, which can be leverage with additional licenses if needed.		

S.No.	Minimum Technical Specification	Bidder's Compliance (Yes/No)	Bidder's Remarks
	Note: Bidders have to ensure 100% Compliance to the below mentioned specifications		
	General Requirements		
1	The proposed solution should provide a single dashboard for physical and virtual Environments		
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR.		
3	The proposed should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions.		
4	The DR Management solution should have a managed lifecycle for all workflows from draft to final published version with version control and time stamp to ensure proper testing and troubleshooting of drill/recovery procedure.		
5	The proposed solution should provide service based dashboard that should provide Business-IT relationship and service availability, DR readiness, Business function availability, etc.		
6	The proposed solution should provide capability to define services, business functions, IT Components and should be able to monitor those from availability standpoint.		
7	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices.		
8	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications.		
DR Monitoring			
1	The proposed solution must offer a workflow based management & monitoring capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts on any deviations.		
2	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness and facilitate policy based actions for events with ability to cancel out polar events.		
3	The proposed solution should allow monitoring basic health parameters for DC & DR components using SNMP		
DR Automation			
1	The proposed solution should provide capable of recovering multiple systems parallel/serial and support inbuilt load balancing techniques for optimized recovery		
2	The proposed solution should be capable of Recovering Servers, Storage, Network, Application, DB, Webserver and Middleware layers on a click of a button		
3	The proposed solution should facilitate Ready to use solution packages for cross platform recovery		
4	The proposed solution should not rely on scripting for recovery automation		
5	The proposed solution should be capable of doing pre-flight checks to ensure conditions are met to ensure a successful DR Drill		
6	The proposed solution should support initiating DR through mobile and it should support IOS, Android, Windows Mobile platform		
7	The proposed solution should support concurrent / parallel application recovery workflows to be executed as part of failover.		
8	The proposed solution should be capable of executing DR drill and recovery workflows in simulation mode, without any changes to DR to ensure conditions are met to ensure a successful execution.		
9	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication		
10	The proposed solution should have flexibility to create custom workflow actions to perform any operation related to virtual guest OS		
11	The proposed solution should be capable of monitoring the firewall policy updates that are happening at production and if any change in the policy is done at DC the same should be identified and replicated across the DR firewall to reflect the respective changes.		
12	The proposed solution should have capability to perform UI, and web automation for various servers and network devices.		
13	The proposed solution should able to conduct DR Drills from a centralized location.		

14	A central console to start, track and configure DR drills for each application.		
15	Out-of-box workflows for switchover and switchback		
16	Details of each drill - including start and end times, status and execution details and DR is ongoing (non-intrusive tests)		
17	Allow running of test while replication between primary and DR is ongoing (non-intrusive tests)		
18	Ability to execute DR drill workflows on Dry-Run/simulation mode to ensure success of actual DR drill by verifying pre-requisites		
19	Should integrate with native OS clusters for drills without the need to replace any of existing native OS clusters.		
20	A central web based console to start, stop and track recovery workflows for each application		
21	Out-of-box workflows for normal copy and failover		
22	Details of each recovery workflow execution detail		
23	Ability to execute DR recovery workflows on Dry-Run/simulation mode to ensure success of actual Disaster Recovery by verifying pre-requisites		
24	Ability to customize and add pre-flight/ dry run checks		
25	A DR aware, flexible and scalable engine to configure, monitor and manage workflows. Has capabilities such as:		
	1. Set environment variables at run time		
	2. Loop, delay, skip, forks & manual input options for workflow execution		
	3. Build/edit workflow using a UI		
	4. Support for parameter passing between actions		
	5. Execute workflow based on user specified schedule/calendar		
26	Recovery operations for popular databases, replications, networking, OS operations		
27	Clear description of operation with settable input parameter values		
28	No programming required to create a workflow		
29	Single console to manage integration of application backup & end-of-day process along with Business Continuity Operations.		
30	Automation scripts and schedules to stop & resume Normal Copy operations before and after nightly backup.		
31	Automation scripts and schedules to stop Normal Copy operations so that end-of-day processing can be done on the database		
Alerts			
1	The solution should be capable of providing DR Dash Board and alerts via email/sms/IVR, mobile App. The dashboard should provide immediate insight into the UIIC's disaster recovery readiness, service availability, and data protection status, as well as the potential impact on business operations.		
2	The proposed solution should provide out of the notification manager to provide alerts through SMS, email, etc. in case of threshold breach or threat of SLA violation		
3	The proposed solution should provide out of the box exception handling manager which may allow taking remedial action in response to certain alerts/alarms		
Reports			
1	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc.		
2	The proposed solution should have good MIS system, especially it should have inbuilt Business level reports to ensure compliance to all types regulations including compliance report submitted to RBI/IBA/ Govt./other regulatory authorites with respect to DR operations and report generator to provide custom reports		
3	Solution should provide a wide array of DR compliance reports that can be generated on demand to help assess and analyze current ability to maintain business continuity.		
4	For each application under software management, the following reports are available:		
	1. RPO deviation over time range		
	2. RTO deviation over time range		
	3. Workflow execution time for each instance		
	4. IRDAmandated BCP/DR reports like BCP testing, DR readiness, application readiness, DR integrity etc		
	5. Replication over time range		
	6. Application summary – configuration & current state		
	7. Test summary report per application		

	8. Provides an exported view of data that can be a data source to popular business reporting engines.		
	9. Audit reports – captures all workflow operations		
5	The proposed solution should provide out of the box reports on RPO deviation, RTO deviation, Datalag, Application DR Readiness status and replication trending		
6	The proposed solution should provide DR drill and audit reports compliant to RBI standard.		
7	The proposed solution should be capable of generating reports in pdf, csv, XML format		
OS & DB Compatibility			
1	The proposed solution must support all major platforms including Linux, Windows, Solaris, HPUX and AIX with native high availability options. It must support both physical and virtual platforms.		
2	The proposed solution must have pre-packaged support for all popular databases Oracle, MSSQL, Sybase, DB2, etc. Support for both physical and virtual platforms should be available		
Replication			
1	The proposed solution should have file level replication for associated application servers and DB log replication which is supported on the commonly used OS platforms and has inbuilt bandwidth compression		
Deployment			
1	The main management server of the proposed should have a mechanism to have a local HA and remote, real time replica to eliminate any single point of failure and should not have any impact on the production in case the main management server fails		
2	The proposed solution should integrate with applications/databases using pre-fabricated API's		
3	The proposed solution should have granular, role based administration and should use existing Active Directory/LDAP, SAML for authentication without the need of its own separate identity management database		
4	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should seamlessly integrate with existing environment without the need to replace/change configuration including existing clusters.		
5	No Production down time should be requested for Installation/integration/configuration of the proposed management Product		
6	The DR management solution should have inbuilt debugging and log capture with facility to view the logs from the web based GUI itself.		
7	The DR Management solution should have a validation tool to verify DC-DR equivalence for OS, databases and applications with both out-of-box and custom templates.		
8	The DR Management solution should be tested and certified by an Accredited Organization to ensure that there are no security vulnerabilities which can be exploited.		
9	The proposed solution should have a file system analytics tool to give total file/directory count, typical scan time, number of open files, time of last replication for a file, file size and time stamp.		
	Monitoring		
1	The tool should have the capability to perform Day-to-day verification of important parameters which could impact DR and alert these changes to respective stakeholders.		
2	Tool should be able to capture, calculate and analyse Recovery Point and Recovery Time monitoring for various applications as per the policy of the UIIC and Provide real-time DR readiness validation.		
3	Tool should be able to capture, calculate and analyse Recovery Point and Recovery Time monitoring for various applications as per the policy of the UIIC. Provide Real time insight into application data loss and recovery time		
4	The tool should keep track of DR Health status on a real time basis. Any changes in the DR Health against different layers like application, database and storage replication should be alerted.		
5	Align DR infrastructure with UIIC's Recovery Time and Recovery Point objectives.		
6	Identify causes of Recovery test failures and Provide recovery workflows to meet service levels & RPO/RTO objectives		
7	A single console to track all of the critical applications real-time recovery readiness. Provision of DR/IT operations manager saves on resources and time and has a 24x7 view of their application DR readiness.		

8	Monitor up/down status & alert on subsystem that are part of a DR solution.		
9	Specific process, services, applications that DR is dependent on are monitored.		
10	Alert (including SMS and e-mail alerts) on adverse conditions that need immediate attention, eliminating potential delay in responding to situations.		
11	Real-time monitoring of application level Recovery Point Objective		
12	Alert when the current recovery point measurement exceeds business set objectives.		
13	Show to management/auditors & regulators that critical applications are meeting their recovery SLA.		
14	Real-time monitoring and status alerts for replication		
15	For each supported DR solution signature, validate pre-build equivalent conditions that are required for successful recovery e.g. For Oracle log - over 40 conditions are validated		
16	Deploy comprehensive DR solution with a few user interface interactions. Eliminate time and efforts required to design and deploy DR solution.		
17	Provide a mapping between primary and DR of applications, servers and replication entities		
18	Map primary to DR assets at a glance, making asset management easy.		
	Event Management		
1	Meet end user specific monitoring needs by raising custom events		
2	Define and register custom event		
3	Raise custom event based on threshold or state conditions		
4	UI page to view and take action on occurred events		
	Discovery & Administration		
1	Relationship map between primary and DR subsystems that make up application’s DR solution		
2	Out-of-box industry best practices DR solutions for popular applications and databases		
3	Support for user roles with different capabilities between operational and administrative role with ability to integrate with AD/LDAP in the environment to eliminate a separate identity management system.		
4	Create and manage user list that are to receive notification via email		
5	The Disaster Drill should be non-intrusive		
6	There should not be any downtime for ATM and IB services during Switch over from DR to DC and switch back from Dr to DC.		
	Replication		
1	Built in file replication software with the following capabilities:		
1.1	1. File replication over IP networks		
1.2	2. Replication from multiple sources to multiple destination files/folders		
1.3	3. Replicate nested files & folders		
1.4	4. Only replicate files that have changed since last replication instance		
1.5	5. Preserves file attributes		
1.6	6. Skip open files		
1.7	7. Provides log of replicated file names, pending files and number of files to be replicated and statistics on throughput		
1.8	8. Ability to specify replication from a point-in-time		
1.9	9. Support replication for Unix symbolic links		
1.10	10. File system analytics tool to give total file/directory count, typical scan time, number of open files, times of last replication for a file, file size and time stamp		
2	Restart replication after a break from last successful replicated point		
3	Replicate only portions of the file that have changed		
4	Specify file/folder names & extensions to include or exclude for replication		
5	On-the-fly file compression for reduced bandwidth usage		
6	Solution should integrate with Storage based replication		
7	Host Based replication		
8	Solution should integrate with Database based replication		
9	Delta resync towards zero data loss.		
	Compliance Requirements		
1	The proposed solution should integrate with the UIIC's Security Information & Event management (SIEM)		

S.No.	Minimum Technical Specification	Bidder's Compliance (Yes/No)	Bidder's Remarks
	Note: Bidders have to ensure 100% Compliance to the below mentioned specifications		
	General Requirements		
1	The solution must be able to perform end-to-end application performance monitoring including OS, Physical, Web, App Servers, DB, App Code. The solution must be able to provide in-depth analysis of problems and determine the root cause.		
2	The solution must be able to provide 24 X 7 performance and high-fidelity data for transaction executed by user of the intended Application(s) from web server to backends		
3	The solution must be able to monitor all infra layers and user transactions with a single agent at OS level. If new JVM's or new Webservers processes are introduced due to load considerations, the agent must be able to auto-detect these and auto instrument with no manual intervention for applications deployed on any OS.		
4	The solution should automatically detect application flow and topology (including changes) along with components involved without any manual configuration.		
5	The monitoring solution should track the performance of all web services and APIs exposed to external partners for every single call made through it and provide detailed performance analysis and root cause for any slowness or failures		
6	The solution should monitor all outbound calls made by the application such as calls to payment gateway, SMS and email gateways and track response times and failures from these calls		
7	The solution must reduce number of false alerts by implementing auto-baselining using percentiles on every user action, methods, DB queries on response times, failure rate and throughput and auto adapt dynamically as the environment changes		
8	The solution should auto-detect when key business transactions aren't working as expected and should be able to provide reports for the same		
9	The solution should provide break up of response time (web, application, database layer times) of maximum possible single transaction, irrespective of whether successful or failed.		
10	It should allow transaction analytics along with actionable reports based on business transactions and should allow to dig deeper into any method or DB statement which may be affecting the performance		
11	The solution should provide interactive and simple web UI for administration, management and monitoring and should not require switching between multiple UI screens and client applications.		
12	The solution must support auto discovery and monitoring of applications deployed in containers without any manual intervention or even changes to container images. The solution must be able to detect if a container has been terminated and automatically detect and start monitoring a replacement container which has been spawned.		
13	The solution should monitor application deployments on public infrastructure such as AWS, Azure, Google Cloud,etc. It should be able to auto detect instance types on these platforms and be able to integrate with native cloud monitoring and event management tools for monitoring of PaaS services on any private or public cloud.		
14	The solution should be able to learn application performance patterns based on different load conditions during weekdays / weekends/ month ends and baseline its performance at different times. The solution should be able to baseline the metrics based on percentile like response time and CPU health etc, and auto-adjust the anomaly thresholds.		
15	The solution should be able to automatically detect any deployment changes in the application code or server configuration and correlate that with the any performance issue. The solution must have facility to integrate with deployment tools, so that these deployment events can be seen along with performance of application in a single monitoring console.		
16	The solution should have an option to store historical data around performance issues, identified root cause, the resolution or workaround done and the events along with the various components of the application were affected over time.		
17	The solution should be able to identify problematic methods and their resource contention, such as CPU thread deadlocks and or network bottlenecks. The solution dashboard should allow to see a breakdown of service execution times at the method level to analyse the failure rates. For eg. In case the issue is related to garbage collection the console should provide relevant metric, based on which the team can tweak the application’s heap memory settings.		
18	The solution should help in monitoring database query executions; it should be able to track and inspects all the SQL statements that the application sends out. The databases should be auto detected and analysed without any manual configuration.		
19	The solution should auto-correlate series of events/alerts and identify the root cause. It should be able to detect and diagnose problems in real time, giving the root cause along with actual lines of code. The system must also provide a replay of the problem evolution which will help developers in doing a post-facto analysis of how the problem evolved over time without waiting for the problem to recur.		
20	The solution must provide reports on the business impact with the details like- number of users impacted, number of applications affected, and service calls impacted due to any problem after reviewing all related events/alerts		
21	For RCA, the solution shouldn’t depend only on time correlation but mainly on the correlation of events across time, processes, hosts, services, applications, and both vertical and horizontal topological aspects of monitored systems		
22	The solution must automatically correlate relevant log messages with any problem that it detects in environment. Relevant log messages that are associated with problems should also be factored into problem root-cause analysis.		

23	The solution must provide diagnostics capabilities like - gain insights into process hotspots which provides break down and filtering data by code execution, network I/O, Disk I/O, Lock time and wait times over times and provide forward and reverse stack traces		
24	The solution must provide process crash details (java,.net, etc..) which should include the signal that killed the process (for e.g., Segmentation fault or Abort), the execution stack frame that crashed and other artifacts like hs_err_pid files, test files that provide analysis of Linux core dumps and other operating systems		
25	The solution must provide a comprehensive list of top exceptions associated with exception class and show the affected services which were impacted. Should show all exception messages with the aggregated stack traces and affected requests		
26	The monitoring solution shouldn't be complicated to use hence it should allow to organize, filter, sort monitored data, for which the monitoring solution must support leveraging tags and metadata information for monitored entities		
27	The solution should collaborate information between Dev/Test environment and Production environment. All relevant information from Production system monitoring problems with their root causes wherever possible should be available to development/test teams so that they don't have to reproduce the problem but are able to quickly arrive at RCA and probable fix		
28	The solution should be able to integrate with CI/CD tools to automate issue detection during QA and testing. It should auto detect regressions and comparing production and dev builds at the code level. It should provide a single dashboard displays the current build status from both the functional and performance perspective.		
29	The solution must be able to integrate with any standard ITSM tools		
30	The solution should be able to provide component back trace to know which component directly call a particular back end and the sequence of preceding component calls leading up to each request all the way back to the browser click or user action that triggered the sequence. It should be able to back trace any component or service request type including database statements, 3rd-party services, and HTTP referrers.		
31	The tool should be able to detect to the extent possible, which of the services and processes suffer from network connection problems. This will enable the operations team to improve the connections between vital infrastructure components. It should be able to provide a clear picture of all inbound and outbound process connections over network interfaces (both physical and virtual).		
32	The tool should allow to understand network topology in the environment at the virtualized network infrastructure layer and know the status of VMs /VLANs). It should also recognize changes within the infrastructure and monitor network interfaces when added.		
33	The solution should be able to monitor the Process-level network capacity on both the host and process level. It should allow to see which process consume the most network bandwidth and have connection problems.		
34	The solution must support creation of custom dashboards using either default or custom metrics. The system must support drill down from dashboards to any individual transactions		
35	Ability to export critical dashboard data and end user experience KPI's to an external solution		
36	The solution should have built-in log analytics, which shall automatically discover log files on the monitored hosts and processes. The team should then be able to pick and choose the Auto-detected logs and to analyse log files. It should allow to filter relevant log files by keywords and time range in a single or multiple log file at once.		
37	The solution must be able to capture entire user journey of a monitored user session, trace it end to end, any performance issues in real time, across multiple digital channels such website, mobile app (IOS/Android), mobile web.		
38	The solution should be able to capture and monitor details about how fast web pages and its components were rendered.		
39	The solution should show how the application is being used by customers across the different channels offered. To enable this for every single user action needs to capture along with username for the monitored user session. This will also give the team the ability to understand why an error is happening. Also Compare bounced user sessions, converted user sessions or new versus returning users to understand the customer base		
40	The solution should be able to capture and provide a session replay of the complete digital experience for user session monitored user across browsers, interfaces, and devices.		
41	The solution should provide recorder to capture and record the business-critical transactions and play back these scripted transactions, including all the screen, keyboard, and mouse interactions that a real user would perform.		
42	The Solution must have synthetic monitoring capabilities and be able to run synthetic (active) / robotic transactions from within the premises and also from Cloud of the vendor to check availability and performance of multi-step transactions over browser (both desktop and mobile).		
43	Solution should be capable of monitoring the end user experience on sampling basis and provide reports accordingly.		
44	The solution should be able to tag the browser side actions to the corresponding server-side service calls in the application stack.		
45	Solution should monitor the impact of response time and availability of third-party object or host currently being used on the website, also quantify the benefits that different CDNs provide in the key geographies.		
46	The solution should be able to monitor the mobile native apps and understand apps crashes. For users accessing the mobile app, the solution must be able to show the platforms and other criteria causing App crash. It should support IOS and Android platforms for monitoring		

47	The solution should have interactive dashboards to compare behaviour and conversions across all channels such as web browsers, mobile devices, operating systems and geographic regions.		
48	The proposed solution should be capable of capturing entire user clicks in the monitored session and allow to readily integrate the collected data (log files). Customer may decide to monitor user sessions (either all or a % of all user sessions) in real time.		
49	The solution should be capable of looking into the details of individual user sessions to understand the difficulties such as slow performance, errors, or application crashes.		
50	The solution should be able to track the performance of each revenue generating component of the web applications, and proactively know if it is affected because of high bounce rate, browser errors, serverside errors or slowness and track each request across all tiers right from web server to back-end, with no gaps or blind spots.		
51	The solution must be able to measure effectiveness of search engine optimization (SEO) on the customer portal and whether any of the search engine BOTS are impacting the portal.		
52	The solution must provide customizable dashboards to track revenue, conversion rates, availability, user experience, drop-off rates and other relevant metrics. The dashboards should be able to show response time of web pages and an indication where users spent most of the time, point at which users dropped out and funnel view with page wise bounce rate. Data should be captured from true end user actions performed either on mobile/desktop browsers		
53	The solution should detect the relevant entry points on the website and help understand the conversions when optimizing performance, such as new campaign pages, product release, help pages etc.		
54	Solution must have capability to pull external log for monitoring.		
55	Solution should have the ability to add devices for monitoring such as WAF / Load Balancer using the exposed API or SNMP. The proposed solution must be able to capture external metrics (KPI's) data exposed by these devices into the APM for centralized reporting.		
	Enterprise Cloud Monitoring		
56	Deploy and configure APM Software to perform Auto-discovery of all stack components and their dependencies		
57	Deploy and configure Full-stack visibility into every process on the monitored host - regardless of the technology		
58	Perform Integration of Application, Host, CPU, Network, Disk, Virtualization, and Cloud within a single model		
59	Ensure Cloud Infrastructure metrics seamlessly combined with application metrics on customers cloud		
60	Perform Auto-injection into all containers (Docker, CRIO, ContainerD, Garden, etc) hosted applications		
61	Expose the necessary Micro-Services to applications as needed		
62	Perform Native integration and instrumentation of PaaS environments & orchestration platforms (K8s, CloudFoundry, OpenShift)		
63	Configure and auto-deploy across entire Kubernetes/Openshift environment using an operator		
64	Configure and auto-deploy across entire Pivotal Cloud Foundry environment using an BOSH add-on		
65	Ensure zero configuration for Real User Monitoring (RUM)		
66	Ensure 100% individual user visibility		
67	Ensure High-fidelity capture of end-to-end transactions - from browser to DB		
68	Design and configure Mainframe end-to-end tracing with code-level visibility into each CICS and IMS service and database statements to DB2 or DL/I		
69	Deploy and configure Fully integrated Synthetic monitoring with public nodes and option for private nodes		
70	Deploy and configure Fully Integrated Session Replay, to replay end user transactions as a video		
71	Deploy, configure, and monitor Fully integrated Log Monitoring with log files automatically discovered for all process and OS		
72	ITSM integration capability- incidents and CMDB such as ServiceNow or any other known solutions		
73	Business communication software integration - interactive chat and alerts such as Slack etc		
74	Deploy and configure a Business Intelligence Solutions integration to export monitoring data to perform business analytics		
75	Deploy and configure Mobile push notifications of problems to relevant stakeholders and manage the distribution list as necessary		
76	Expose API with the ability to push data in and pull data out		
	Business Analytics		
77	Design, develop and Configure Custom/Definable Business conversion goals		
78	Ensure Full capture of authenticated usernames for 100% users		
79	Capture business KPIs from within user's browser		
80	Capture business KPIs from backend application method calls		
81	Complete capture of entry/exit page analytics		
82	Browser/Device/Location Analytics for 100% users		
83	Design and develop Conversion funnel visuals		
84	Ensure Easy deployment of packaged business dashboards via API		
85	Enable, configure and deploy Automatic detection of user frustration, e.g., Rage Clicks		
86	Configure and deploy Automatic bounce rate detection		
87	Integrate and enhance through web analytics solutions such as Google Analytics, Adobe Analytics		

88	Ensure the system captures Automatic detection of user types (New vs. Returning Users)		
	AIOPS		
89	Configure the Self-learning AI to automatically locate problem inflicting components and identify root causes		
90	The AI / ML engine should be able consume data across multiple applications and infrastructure component to isolate the area of problem		
91	The AI engine should be able to consume any agent-based data or custom-data, or custom event sent to the platform as part of the root cause analysis		
92	The AI engine should not require any additonal manual configration of the rules or custom thresholds for identifying problem areas		
93	The platform should allow to predict user load based on past data		
94	Configure to Automatically eliminate alerts storms		
95	Develop and configure the Full replay of problem lifecycle for post-mortem analysis		
96	Enable Automatic determination of business impact related to detected problems		
97	Enable Automatic changepoint detection of all 1st and 3rd party metrics		
98	Should have Expert knowledge built-in to identify top findings and recommended optimizations		
99	Should design and deploy Query language for customized analytics		
100	Enable AI-powered VoiceOps (natural language interface) and ChatOps		
101	Should configure the system to be Able to ingest and process (with A.I.) data & events from external tools		
102	Reduce need for manually correlating dashboards		
	Application Security		
103	Full visibility: Find all runtime vulnerabilities in your environment		
104	Full context: See all affected processes including related services, applications and hosts, as well as Kubernetes workloads, nodes and clusters		
105	The platform should allow for Application Security with additional agents or overhead		
106	Automated risk assessment: Understand network exposure, which data is at risk, and how easily vulnerabilities can be exploited by an attacker		
107	Drive automation use cases and access all security findings with full details via API		
	Digital Experience Monitoring		
108	By instrumenting apps with APM Software, OICL get full visibility into active users, sessions, web request performance, and application crashes		
109	Instrument your mobile apps to gain full visibility into the experience of your mobile app users.		
110	Receive mobile-app crash alerts and monitor the performance and usability of your apps directly on users' devices.		
111	Monitor the global distribution of your mobile apps and keep a close eye on important usage and quality metrics following new version deployments.		

S.No.	Minimum Technical Specification	Bidder's Compliance (Yes/No)	Bidder's Remarks
Note: Bidders have to ensure 100% Compliance to the below mentioned specifications			
	AI and Intelligent Virtual Agents		
1	Use of Machine Learning/Artificial Intelligence/Speech to Text /Natural language Understanding in IVA Transactional Capability		
2	Deployment Option On-Premise / Cloud		
3	Integration with Telephony / IVR platform for voice enabled human voice conversations		
4	Options to send Customer links with Virtual Agent Guidance for uploading Issue related Images		
5	Capability to integrate with Digital Channels like IVR, Webchat, What's app, Agent screens, backend systems like CRM using APIs, Web Services, Custom Adapters etc		
6	Text to speech and speech to text conversion and NLP Engine		
7	Multi Language Support, integration with translation services		
8	Micro service architecture and Scalability for enhanced add-on Services.		
9	Industry Compliance and Security Capabilities like AES256 encryption, data privacy, SAML/SSO, multi factor authentication		
10	Post deployment ready to provide skilled manpower for proactive monitoring, technical and functional support.		
11	Ability to handle the exceptions based on the business rule such as frustration based, intent based, scheduled when the chatbot is unable to process request after specified attempts etc.		
12	Sentimental Analysis and Service Level Analytics		
13	Agent Screen Option		
14	Agent assist / Knowledge Based search		
15	Platform option administrator for Training the BOT		
16	UI based interface to create new flows as per requirements		
17	Easy to use Widgets for Location, Flow creation, Input options, voice / text options		
	Unified Communication Functionalities		
1	Same Unified Communications (UC) client that provides users with real time collaboration capabilities		
2	Support for Windows and MaC OS		
3	Support for Android and iOS devices Smartphones		
4	The Softphone should provide full call control from an iPhone or Android powered smartphone.		
5	Make and receive phone calls and instant messages, host and attend audio conferences.		
6	See employee availability via presence, and use Geo-tracking to determine the location in the field.		
7	All of this is done using the corporate directory, so there are no personal cell phone numbers will be involved.		
8	The Softphone application should be downloadable from Google Playstore or Apple iTunes without any additional cost for any number of device.		
9	Solution should provide a "presence" application for users, so that they can see the availability status of their contacts in their contact list.		
10	The common supported status for this application should be available, busy, idle, away etc.		
11	The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND) etc.		
12	Shall provide support for open protocols like XMPP.		
	Reporting		
1	Platform should support Unified Multi ChannelReal-time and Historical Reporting and pre defined real time and historical reports.		
2	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes		

3	Platform should support various built in historical report types including daily, weekly, monthly, skillset, Agents, abandoned contacts, overflow contacts, threshold exceeded contacts, contact classification, source of disconnect, email report, system status.		
4	It should also support real time dashboard for supervisors and agents if required to display agent specific metrics.		
5	Platform should have 45+ built-in out of the box report including call by call report, contact summary report, agent performance report.		
6	Platform should also include custom report creation web based tool to create and edit the reports.		
7	Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV		

S.No.	Minimum Technical Specification	Bidder's Compliance (Yes/No)	Bidder's Remarks
Note: Bidders have to ensure 100% Compliance to the below mentioned specifications			
Data Privacy			
1	Data privacy and compliance to the current national IT Act and Data protection Act		
2	Can the solution be compliant with GDPR requirements?		
General			
3	The product supports REST based APIs for integration		
4	The product supports fully-hosted solution		
5	The product supports branding capabilities		
6	The prouct supports common integration standards (i.e., OpenID Connect, OAuth, SAML)		
7	The applicant's experience of building and successfully deploying solution(s) with distributed ledger or blockchain		
8	Kuppingercole, Gartner, Forresster		
9	BFSI preferable		
Identity Proofing			
10	The product provides the ability to verify physical presence of the user, the authenticitiy and validitity of the user's government documentation, and the identity attributes gathered from the documentation to achieve a high degree of identity assurance for the user.		
11	The identity proofing solution supports the capture of data from passports from all major global regions (Americas, EMEA, APAC, Latin America)		
12	The identity proofing solution supports the capture of data from identity cards (non-driver's licenses) from all major global regions (Americas, EMEA, APAC, Latin America)		
13	The product provides the ability to integrate with third-party organizations for additional verification (e.g., credit bureaus, KYC, utility company bills etc.)		
14	The product provides the ability to integrate with the vendor's customer organizations for additional verification (e.g. from their customer's Active Directory or user databases)		
15	The product provides the ability to send OTP to verify identity		
16	The product provides the ability to generate a numeric indicator of trust about the identity being verified.		
Orchestration			
17	Ability to interface with enterprise SIEM solution to transfer logs from IAM systems		
18	Ability to communicate/interact using REST protocol		
19	Ability to communicate/interact using LDAP		
20	Ability to support coexistence of multiple Access Management and Federation solution in an organization during a state of transition		
21	Ability to support migration of applications (with minimal application code changes) from legacy Access Management (eg. Header based authn) to Federation solution (eg. SAML, OpenID Connnect)		
22	Ability to support federation to multiple IDP's and act as a SP		
Passowordless Authentication			
23	The product should allow the user to login to the workstation OS desktop in less than 7 seconds.		
24	The solution supports biometric authentication factors, including fingerprint, facial, and voice authentication		
25	The user should only need to perform a minimum number of actions (i.e. unlock a phone, open an app, authenticate to the app, select a resource, etc.) to achieve login at the OS level or to an application.		
26	Provide the ability for the user to leverage a mobile device to authenticate to the target resource - desktop or web application - using multiple factors for authentication		
27	The solution supports FIDO2-compliant non-mobile devices (e.g. U2F tokens, SmartCards, etc.) for authenticating to OS logins and web applications		
28	The solution needs to support desktop logins and integrate with single sign-on solutions for enterprise use cases.		

29	The solution needs to support web-based application logins and transaction verification use cases for remote/3rd party users.		
30	Native plugins, OOTB connectors or APIs are available for leading IAM tools (e.g. Okta, ForgeRock, Ping, AD, and Broadcomm SiteMinder) as part of the solution suite.		
31	This is important for a transformation/migration perspective – Ability to integrate a passwordless product into the multiple internal SSO solutions and use that consistent user experience to make technology rationalization moves in the backend and avoid user impact.		
32	Ability to offer offline authentication methods in an event the user's workstation and/or authenticator does not have network connectivity to the authentication server		
33	The product offers the ability for client-facing Brand Control - All Functionality Offered in a Branded Application or Full White Label SDK Deployment		
34	Register the user with the password-less credential under 30 seconds		
35	The product supports push-based authentication requets to a user's mobile device to authenticate the user and request authorization of a business function or transaction		
36	Ability to use Windows credentials to establish a Kerberos SSO Session by using the password-less desktop authentication? This is, again, both a security and a UX requirement.		
37	Ability to use Mac credentials to establish a Kerberos SSO Session by using the password-less desktop authentication? This is, again, both a security and a UX requirement.		
38	The solution has out-of-box integrations with AD to provide a multi-factor authentication capability		
39	Solution can integrate with on-premises Active Directory for user authentication		
40	Vendor provides a SaaS option for password-less authentication		
41	Is the desktop login technology FIDO2-compliant, removing shared secrets between the phone and desktop. This is an architecture/design requirement.		
42	Is the desktop login technology FIDO2-compliant, removing shared secrets between the phone and desktop. This is an architecture/design requirement.		
43	The solution can provide a FIDO2-compliant login method for VPN logins		
44	The solution can provide a FIDO2-compliant login method for Virtual Desktop Interface (VDI) logins		
45	The product is able to detect 3-dimensional liveness without specialized cameras.		
46	The product is able to detect 2-dimensional and synthentic digital images presented to the authentication device's cameara.		
47	The product provides a gesture-based ability (i.e. facial expressions, head turning, etc.) to validate the liveness of the user.		
48	The product is resilient against attempts to inject a synthetic biometric factor (e.g. a digital face, fingerprint, or voice) in an attempt to spoof a real user's identity.		
49	The product is resilient against attempts to reply the authentication exchange between the authenticator and the server in an attempt to spoof a real authentication challenge/response.		
50	The product is resilient against attempts to inject synthentic video and/or audio to the authentication algorithm in an attempt to spoof the user's identity.		
51	The password-less authentication technology is able to run on the iOS Platform		
52	The password-less authentication technology is able to run on the Android Platform		
53	The product is provided as an SDK for seamless embedding into an organization's business application.		
Security			

54	The product supports verification and incorporation of identity attributes provided by the user through self-sovereign identity attribute exchange on the blockchain, W3C standards, DID protocols and Blockchain (not storing data but public keys) in mind? Please add the details in the presentation/ technical details link		
55	Built the solution based on peer to peer distributed data sharing ecosystem		
56	Protection against various attacks, data protection, access mechanism, protection, detection and action and recovery scenarios		
57	Identity Assurance and Authenticatoin Assurance as per NIST 800-63-3 Standards		
58	Data should reside in Datacenters hosted in India		
Support Center			
59	The vendor should have suport center in India		

S.No.	Particulars	Bidder Score (Yes/No)	Bidder's Comments (BC)
1	**Hardware Specifications**		
1.1	The Proposed Solution must be Hardware Appliance based.		
1.2	The Proposed Solution should have Guaranteed 5-year Platform lifespan.		
1.3	The Proposed Solution must have redundant power supply.		
1.4	The Load Balancer Proposed should have at least 16x 10GE SFP+ and 4x 40GE SFP+ and all ports should be populated from day one		
2	**Traffic Redirection**		
2.1	The Proposed Solution should support Server Load balancing.		
2.2	The Proposed Solution (ADC) should support minimum 20 Gbps throughput with scalability of 80 Gbps throughput without changing / adding hardware		
2.3	The Proposed Solution must have performing load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.		
2.4	The Proposed Solution must have load balancing based on least connections, Hashing, Persistency based (Cookie, Client IP, SSL ID etc.)		
2.5	The Proposed Solution must have the ability to enable and disables server gracefully and hard shutdown.		
2.6	The Proposed Solution must have HTTP 2.0 gateway.		
2.7	Proposed solution should support 1.5 million layer 7 request per second		
3	**Persistency**		
3.1	The Proposed Solution must have session persistency based on Layer 3, Layer 4 and Layer L7 information		
4	**Health Monitoring**		
4.1	The Proposed Solution must have the ability configure TCP and UDP health check for real web servers as well as health check at Application, Data Base level in native DB query format. The Proposed Solution must have support creating application specify custom health check using scripts.		
5	**Virtualized load balancer should have complete virtual infrastructure to support:**		
5.1	Fault isolation between each virtual load balancer instances		
5.2	Resource reservation between each virtual load balancer instances		
5.3	Upgrade of OS on any virtual load balancer should not affect other		
5.4	Solution must have atleast 20 Active configured Load Balancer Instances, scalable up to 25 without changing / addting hardware		
6	**SSL Acceleration and Central**		
6.1	The Proposed Solution must have SSL offload - the ability to manage client side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text.		
6.2	The Proposed Solution Should support minimum 20K SSL Transactions per second for 2048 bit key and scalable up to 60K SSL Transactions per Second for 2048 bit key. One TPS equal to one CPS		
6.3	The Proposed Solution should support minimum SSL throughput of 15 Gbps and should be scalable up to 40 Gbps & above		
6.4	The proposed solution should support 4K certificates without changing the appliance or software		
7	**HTTP Compression**		
7.1	The Proposed Solution Should support minimum 5 Gbps with scalability 10Gbps of compression throughput & Caching functionality to Cache static and Dynamic content		
7.2	The Proposed Solution should Selective compression to avoid know compression problems in commonly used browsers		
8	**Data Center Automation and Orchestration**		
8.1	API based SDK/XML-RPC/REST API to integrate with proprietary/open management systems and centralized management tool need to be provided by OEM		
9	**Global Server Load Balancing**		
9.1	The Proposed Solution must have Global Server Load Balancing supported on the same appliance		

S.No.	Particulars	Bidder Score (Yes/No)	Bidder's Comments (BC)
9.2	The Proposed Solution must have performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.		
10	**Mobile Stream Optimization**		
10.1	The Proposed Solution should be Reducing the number of requests required for rendering each page.		
10.2	The Proposed Solution should be Reducing the number of bytes in page responses.		
10.3	The Proposed Solution should be Simplifying and optimizing the content served to the client browser.		
11	**Performance Monitoring**		
11.1	The Proposed Solution Should be able to monitor more than 1000 Req/Sec		
11.2	The Proposed Solution should be Identifying the root cause of slow performance issues		
11.3	The Proposed Solution Monitoring Cache Server Performance		
11.4	The propsoed solution should display the usage of web application across different geographical location of branches		
12	**Clustering Redundancy**		
12.1	All nodes in the Cluster are in Use		
12.2	All Nodes in the cluster must take Traffic simultanoeusly for all VIP Traffic		
12.3	New Nodes can leave and join the cluster without impacting existing connections		
12.4	Any node is capable of taking over the responsibility of another node in the event of failure.		
12.5	Cluster can be formed with 2 to 32 nodes		
12.6	Dynamic Changes Permitted in Run time.		
12.7	Nodes can be placed in different racks over L2		
12.8	Built-In fault Tolerance (System should provide inherent reliability. If a node fails or becomes unreachable, the traffic handled by that node is automatically redistributed to the remaining active nodes through the normal traffic distribution mechanism)		
12.9	Remains single system image for configuration and management		
13	**Management and Reporting**		
13.1	The Proposed Solution must have Web Based Management for full device configuration (GUI)		
13.2	The Proposed Solution must have modifying configuration via modular CLI		
13.3	The Proposed Solution must have SSH and HTTPS access		
13.4	System enables to send logs to another server via Syslog		
13.5	The Proposed Solution must have diagnostics which are readily available and easy to send to support (capture core dumps, configurations, logs, and so on).		
13.6	The Proposed Solution must have Out of Box management.		
13.7	The Proposed Solution must provide SSL Traffic Visibility through Dashboards		
13.8	Service ,Support & Training		
13.9	The proposed solution must have centralized Management, Monitorining, Auditing and Reporting Tool		
13.10	The devices and software should be supported by the OEM on a 24x7 basis through a global Technical Assistance Center (TAC). The support should be provided direct from OEM and not through any intermediate third-party.		
13.11	Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity & dynamic detect.		
13.12	The Proposed Solution must have Out of Box management.		
13.13	The Proposed Solution must provide SSL Traffic Visibility through Dashboards		
13.14	Service ,Support & Training		
13.15	The proposed solution must have centralized Management, Monitorining, Auditing and Reporting Tool		

S.No.	Particulars	Bidder Score (Yes/No)	Bidder's Comments (BC)
13.16	ADC on same Appliance and should be in Gartner Leaders Quadrant / among top 5 Vendors for ADC in IDC as per the latest last 2 reports available.		
13.17	The devices and software should be supported by the OEM on a 24x7 basis through a global Technical Assistance Center (TAC). The support should be provided direct from OEM and not through any intermediate third-party.		
14	Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity & dynamic detect.		
15	Solution must support SSL VPN features along with SSO. The Solution must also provide machine authentication based on combination of parameters like HDD ID, CPU info, OS related parameters i.e. MAC address to provide secure access to corporate resources.		
16	The overall Solution must support SAML based Authentication for Apps.		

Sl.no	Activity / Stakeholders	Agent	Customer	Corporate Customer	Broker	Web aggregator	Motor Dealer	Employee	Pensioner	Surveyor	Advocate	Investigator	Admin Users	TPA
1	login and view customised dashboard	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Change password after login	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
3	update email id	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
4	update mobile number	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
5	New policy purchase	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
6	policy renewal	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
7	pay premium online	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
8	register the policy on portal	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
9	View all previous policies in dashboard	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	Y
10	print the policies/ endorsement	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	N
11	download proposal form	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N
12	intimate a claim on policy	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	Y
13	View status of the claim	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
14	download claim form	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
15	upload claim form	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
16	upload document	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
17	upload photographs	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
18	upload video / audio files	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
19	View premium procured	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N
20	view commission earned	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N
21	View list of policies due for renewal	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
22	View List of all claims on policies purchased	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	Y
23	View Circulars	N	N	N	N	N	N	Y	Y	N	N	N	N	N
24	View Product info	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
25	View user specific content	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
26	add content	N	N	N	N	N	N	N	N	N	N	N	Y	N
27	modify content	N	N	N	N	N	N	N	N	N	N	N	Y	N
28	delete content	N	N	N	N	N	N	N	N	N	N	N	Y	N
29	Report Grievance	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N
30	Update Grievance	N	N	N	N	N	N	N	N	N	N	N	Y	N
31	View status of grievance	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N
32	create user	N	N	N	N	N	N	N	N	N	N	N	Y	N
33	update other user mobile no/ email / password	N	N	N	N	N	N	N	N	N	N	N	Y	N
34	Delete user	N	N	N	N	N	N	N	N	N	N	N	Y	N
35	Assign Privileges to users	N	N	N	N	N	N	N	N	N	N	N	Y	N
36	Create office master	N	N	N	N	N	N	N	N	N	N	N	Y	N
37	update office master record	N	N	N	N	N	N	N	N	N	N	N	Y	N
38	delete office master record	N	N	N	N	N	N	N	N	N	N	N	Y	N
39	Upload TPA data	N	N	N	N	N	N	N	N	N	N	N	N	Y
40	Download Policy, Claim and Log data	N	N	N	N	N	N	N	N	N	N	N	N	Y