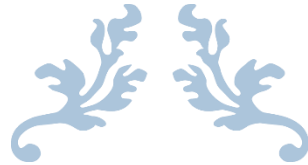


Request for Proposal



Selection of System Integrator for Development and Implementation of Transaction Management and Claim Processing System for Biju Swasthya Kalyan Yojana (BSKY)

RFP Ref. No.: OCAC-SEGP-SPD-0025-2022-22059



Vol-II | Terms of Reference



ODISHA COMPUTER APPLICATION CENTRE

[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]

OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India

W: www.ocac.in | T: 0674-2567295/2567283 | F: 0674-2567842

Table of Contents

1	Background	7
1.1	About BSKY scheme	7
1.2	Stakeholder	7
1.3	About the existing BSKY Application	7
1.3.1	Modules available	8
1.3.2	Technology	8
1.4	Objective	9
2	Scope of work	9
2.1	Overview	9
2.2	Management of existing BSKY application	10
2.2.1	Handover and Takeover	10
2.2.2	Ensure continuity of the existing application	11
2.3	Requirement Study	12
2.4	Design	12
2.5	Development	12
2.6	Integration	13
2.6.1	Private Hospital's Integration	13
2.6.2	Other applications	13
2.7	Testing	14
2.8	Third Party Audit	15
2.9	SSL Certification	15
2.10	Training	15
2.11	Online Help / Reference with Search Option	16
2.12	Supply of tools and license	16
2.13	Deployment & Configuration	16
2.14	UAT & Go-Live	17
2.15	Data Migration	17
2.16	Infrastructure Support	18
2.16.1	Implementing Software & Tools	18
2.16.2	Business Continuity Planning	18
2.16.3	Documentation	18
2.17	Call Centre Operations	19

2.18	Technical Support Unit	19
2.18.1	State Level	19
2.18.2	Districts in Odisha.....	20
2.18.3	Major Cities in India	21
2.19	Operation & Maintenance.....	22
2.19.1	Application Support.....	22
2.19.2	Software Maintenance.....	22
2.19.3	System/Infra Support	23
2.19.3.1	Database Administration.....	23
2.19.3.2	Server Administration	23
2.19.3.3	Security Administration.....	24
2.19.3.4	Backup & Restore Management	24
2.19.3.5	System / Network Administration.....	24
2.20	Project Management	24
2.21	Guiding Principles	24
2.21.1	Standards.....	24
2.21.2	Application	25
2.21.3	Integration.....	25
2.21.4	Data	25
2.21.5	Data Security	25
2.22	Adherence to Standards	25
2.23	Security, Integrity & Confidentiality	26
2.24	Change Management Team	27
2.25	Exit Plan	28
2.26	Project Documentation	29
2.27	Expected Deployment of Personnel	29
2.28	Expected Project Timeline	30
2.28.1	Timeline for managing the existing BSKY application.....	30
2.28.2	Timeline for the New BSKY 2.0 application.....	31
2.28.3	Timeline for IaaS and PaaS (Oracle ExaCC)	32
2.29	Service Level & Penalty.....	32
2.29.1	New BSKY 2.0 Application	33
2.29.2	IaaS and PaaS.....	33

2.29.3	Waiver of Penalty	34
2.30	Bill of Material & Quantity.....	34
2.31	Payment Terms	36
2.31.1	Management of existing BSKY application	36
2.31.2	Implementation of New BSKY 2.0 application	36
2.31.3	OEM License	37
2.31.4	IaaS and PaaS.....	37
2.31.5	Recurring Expenses	38
2.31.6	General Conditions.....	38
3	Functional Requirements of BSKY 2.0	39
3.1	User & Master Management.....	39
3.2	Hospital Registration	41
3.3	Transaction Management System.....	42
3.4	Claim Management System.....	44
3.5	Development of Mobile Application	45
3.6	Dashboard & MIS.....	45
3.7	Grievance Management	46
3.8	Self Service.....	46
3.9	General Features	47
3.9.1	Web Design Considerations	47
3.9.2	SMS and Email Facility.....	47
3.9.3	Data Export and Import Facility	47
3.10	Use of Emerging Technology	47
3.10.1	Analytics and Reports.....	47
3.10.2	Middleware Tool	49
3.10.3	Integration Tool.....	49
3.10.4	Data Encryption and Security Tool.....	52
3.10.4.1	File and Database level Encryption	52
3.10.4.2	Data Protection for Database.....	53
3.10.4.3	Vulnerability Assessment	58
3.11	Requirement of IaaS and PaaS	58
3.11.1	Supply and Installation of Hardware Infra	59
3.11.2	Managed Services & Technical Support.....	59

3.11.3 Bill of Material and Technical Specifications 60
3.11.4 Bill of Material of ORACLE License available with OCAC 69

Abbreviations

BSKY	Biju Swasthya Kalyan Yojana
BSKY 2.0	New Biju Swasthya Kalyan Yojana wherein all the beneficiaries of NFSA/SFSS are included under new scheme
CPD	Claim Processing Doctor(s)
FAQ	Frequently Asked Question
FRS	Functional requirement specification
H&FW	Health & Family Welfare Department
IaaS	Infrastructure as a Service
iFMS	Integrated Finance Management System
LGD	Local government directory
OCAC	Odisha Computer Application Centre
OSDC	Odisha State data Centre
PaaS	Platform as a service
PFMS	Public Financial Management System
RFP	Request For Proposal
SNA	State Nodal Agency
SHAS	State Health Assurance Society
SI	System Integrator
SRS	Software requirement Specification Document
SPDP	Social Protection Delivery Platform
UAT	User Acceptance Test

1 Background

1.1 About BSKY scheme

Biju Swasthya Kalyan Yojana (BSKY) aims to provide Health coverage to eligible Households of Odisha especially the economically vulnerable sections. Families having BSKY Health Card can avail cashless treatment at any empaneled private hospital under BSKY within or outside the State. Card holder families can avail facilities such as registration, consultation, medical tests, pathologies, treatment, IPD and follow-up consultation for which State Government will bear the cost up to the annual coverage amount.

State Government bear the full cost of all healthcare services delivered to all patients in all State Government health care facilities starting from Sub Centre level to District Head Quarters and Government Medical College Hospital level and State Government bear the cost of healthcare services provided in the empaneled private hospitals for BSKY card holder families in the State, for an annual health coverage of Rs. 5,00,000/- per family and additional Rs. 5 lakh for the women members of the family.

1.2 Stakeholder

<i>Stakeholders</i>	<i>Roles</i>
Department/SHA	Define polices, process, packages, etc
Hospitals	Raise Claims, update daily transaction, maintain discharge information, etc.
Claim Processing Doctors	verify and approve/ reject/ forward the Claims raised by Hospital
SNA Doctors	Verify and approve/ reject/ forward/ revert the Claims raised by Hospital.

1.3 About the existing BSKY Application

State Health Assurance Society (SHAS) has already implemented IT system to discharge its services and help the entitled beneficiary to receive Health Coverage from the scheme. The purpose of the application is to automate the transaction and claim process at hospital and ensure smooth monitoring of the implementation of the existing scheme. The existing application has been implemented across all the empaneled hospitals and majorly used by departmental users, hospital users, CPD doctors, SNA doctors. The existing application was implemented to provide following services.

- a) Enhance the responsiveness of SHAS through workflow automation
- b) Enhance the ease and convenience of stakeholders in accessing the information and services provided by SHAS

- c) Increase efficiency, transparency and accountability of SHAS in administering the “Biju Swasthya Kalyan Yojana”
- d) Implement the cashless treatment service at the point of service.

1.3.1 Modules available

Transaction Management System	Through this module patient information get validated using connected POS. The user can get information on the card balance and necessary information captured while discharging of patient.
Package management	Through this module addition and modification of Package can be done by the concerned user
Pre- Authorization Management	This is the vital module of the system where in the pre authorization process is managed by the concerned authority
Hospital Management System	All empaneled hospital information captured through this system
Claim Management System	This module is implemented to capture the claim information process through which the CPD doctors & SNA doctors verifies the claim process received at client end

1.3.2 Technology

The existing BSKY application is developed in Microsoft .net technology with database as MS Access and SQL server. The application is hosted at State datacenter and the technical stacks are as per below;

Web Application Framework	ASP. NET 2.0
Database Server	MS Access, SQL Server 2012
Server Operating System	Windows server

The major challenges with the existing application are, like few of the modules were developed in web version and few were developed in desktop version which created hindrances while updating the information of a beneficiary. As the application was developed in 2 different versions, syncing of data on a daily basis is also a major challenge. Thus delay occurred on the daily transaction conducted at hospital end, to update the information in the system. Looking at these challenges, the department envisaged to develop BSKY2.0 application to enhance the business process of BSKY Scheme.

1.4 Objective

Odisha Computer Application Centre (OCAC), the Designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, has evolved through years as a center of excellence in Training, IT solutions and e-Governance. It has contributed significantly to the steady growth of IT in the state. OCAC on behalf of Health and Family Welfare Department, Govt. of Odisha intends to implement BSKY 2.0, a comprehensive solution that includes overall management from Hospital empanelment to patient verification, treatment and treatment claim and approval process for empaneled hospitals and is pleased to engage qualified and preferred software development Agency to execute this project for development, testing, implementation and maintenance of BSKY 2.0. The main objectives of the proposed IT system are as follows:

- a) Provide healthcare facilities to the economically weaker section of society.
- b) To ensure adequate, qualitative, preventive and curative health care to people of the State.
- c) To ensure health care services to all particularly to the disadvantaged groups like scheduled tribes, scheduled castes and back ward classes.
- d) To reduce the transaction process time by adopting fully web based application
- e) To generate various insightful reports which will help the concerned stakeholders on the implementation process of the scheme
- f) To reduce approval time by strengthening the processes

2 Scope of work

2.1 Overview

- a) Transition plan and smooth knowledge transfer of entire BSKY application from existing SI by complete takeover of application in As-is condition along with all developments, enhancements, databases, source codes, user manuals, system documents, design documents, integrations, infrastructure at OSDC till moving application to the new environment.
- b) Application Maintenance and Support of the both existing software and to be developed software. The scope shall include complete technical and operational support for application software, system software and other computing infrastructure procured under this project.
- c) Study, development and implementation of new application modules as per the requirement of this RFP

- d) Application of analytics on transaction data to provide insights and analytical reports such as suspect or fraud analysis, forecasting with anomaly detection etc.
- e) Integration with the empaneled private hospital's application
- f) Other API based integration such as third-party application/utility
- g) Set-up and operation of Helpdesk which will provide technical and functional support to the stakeholders such hospitals, department, doctors, etc on 24X7 basis.
- h) Deployment of support personnel at District headquarter and major cities outside Odisha for support of empanelled hospitals under BSKY.
- i) Supply and installation of ORACLE ExaCC hardware at OSDC
- j) Operation, management and support of the application for a period of 3 years from date of Go-live which may be extended further for another 2 years depending upon requirement.

(The bidder should furnish un-priced Bill of Materials along with Technical Bid which should cover software application, system software, hardware, resources etc.)

2.2 Management of existing BSKY application

The primary objective is to ensure the continuity of the existing application for a period as defined in this document from the date of the onboarding of new SI. The new SI will be responsible for smooth transitioning of the entire application, infrastructure, and services from the incumbent SI ensuring business continuity and performance. As part of the transition, the new SI is also responsible for providing necessary compute & storage infrastructure on the cloud/premise including the underlying software licenses/certificates to host the Application.

2.2.1 Handover and Takeover

The new SI will perform all the functions and services necessary to accomplish the Transition of the entire knowledgebase, application (Web, Handheld device, other utility and integrations etc.), infrastructure, and services under existing BSKY application from the existing SI on or before the specified completion dates. New SI will be responsible for the overall management of the transition in accordance with the transition plan and will work to ensure the transition is completed on schedule and to identify and resolve any problems encountered. Further the new SI will demonstrate its understanding of existing BSKY application and ability to support to reasonable satisfaction of the officials, prior to the completion of Transition Phase, proving that it is ready to take over independently.

The responsibility of the new SI during the knowledge transfer phase includes following.

- a) Submit a detailed Knowledge Transfer plan at the start of the KT phase, listing all the activities from their end, including the expectations from existing SI and the officials.
- b) Preparation of a checklist (as part of knowledge transfer plan) to ensure proper knowledge transfer. This shall be reviewed and subject to approval by the officials.
- c) The knowledge transfer shall include initial and ongoing training on existing BSKY application, training materials, operations manuals, procedure manuals, source code control and deployment/ installation guide.
- d) During the handover phase the new SI will be given a hands-on exposure to existing BSKY application by the incumbent SI. During this phase, the new SI will be in shadow and all communication will be done by the existing SI.
- e) Post-handover phase, the new SI shall take over the entire responsibilities of existing BSKY application for a defined period as mentioned in this document, however the existing SI shall deploy its team as a shadow to support and will be responsible for supervising and reviewing all the activities of the new SI.
- f) Any change request received during this phase shall be implemented by the Incumbent SI
- g) The new SI shall validate the inventory of all project related assets (H/w & S/w) as submitted by the existing SI
- h) The new SI shall prepare the functional, system, technical and process documentation of the existing applications and processes necessary for continued operation and maintenance of the services

2.2.2 Ensure continuity of the existing application

During this period, the new SI shall undertake following scope of services:

- a) Ensuring the continuity of existing BSKY application by complete takeover of application, infrastructure at SDC, in as-is condition along with all developments, enhancements, databases, source codes, user manual, system study document, design documents, integrations and all other components required to run the system effectively without any interruption.
- b) Standard application maintenance support and user training
- c) Bugs / Issues fixing in the application software as well as operational problems
- d) Tuning and code changes for optimal performance
- e) Periodic testing and security audit of the application as per the OSDC protocol
- f) Changes in the report / creation of new reports as per the requirement

g) System administration, Data validation/correction, etc

2.3 Requirement Study

The new SI shall perform a detailed assessment of the service and solution requirements of each participating department as mentioned in this section. Based on the assessment, the new SI shall develop & finalize the Functional Requirements Specifications (FRS) and the System Requirement Specifications (SRS). While doing so, it is suggested that the new SI should:

- Consult with SHAS team, OCAC and Health & Family Welfare Department officials
- Engage some domain experts during the study
- Follow standardized template for requirements capturing
- Maintain traceability matrix from SRS stage for the entire implementation
- Visit some empanelled hospital to listen the issue in the existing application and new requirements, if any.

Any additional functionalities/modules relevant to the scope of BSKY 2.0 application identified during the business process requirement study shall also be considered as part of new SI scope of work.

2.4 Design

The new SI shall design the solution architecture and specifications for meeting the requirements mentioned as part of this document. The new SI shall be entirely responsible for the design and architecture of the system implemented to satisfy all requirements as described in this document including sizing of the required hardware.

2.5 Development

The new SI shall identify, design and develop components / functionalities that are required to address the proposed application requirements mentioned in this RFP. The new SI shall supply the following documents along with the developed components:

- Business process guides
- Data model descriptions
- Sample reports
- Frequently asked question (FAQ) guides
- Any other documentation required for usage of implemented solution

The new SI shall implement a system for monitoring the SLAs and ensure that the system addresses all the SLA measurement requirements and calculation of applicable penalties as indicated in the document.

2.6 Integration

2.6.1 Private Hospital's Integration

The new SI is responsible to integrate the new application with the empaneled Private Hospitals having existing application for smooth transaction process. The department will facilitate with the empaneled hospitals for sharing of required APIs/ web services which will be used for the applications.

2.6.2 Other applications

Following applications will be integrated with the proposed solution. The new SI should make necessary effort by visiting the respective department to understand the following applications to be integrated.

SI#	Name of the Application	User Department	Purpose of Integration
a)	National Food Security Act (NFSA) / State Food Security Scheme (SFSS):	FS&CW Department, Govt. of Odisha	To identify the eligible Beneficiaries
b)	Aadhaar Authentication Framework	E&IT Department, Govt. of Odisha	
c)	Social Protection Delivery Platform (SPDP)	Finance/E&IT Department, Govt. of Odisha	
d)	State Dashboard	E&IT Department, Govt. of Odisha	To display the scheme performance as per the defined KPI
e)	BSKY Card Issuance System	E&IT Department, Govt. of Odisha	To capture the card information in the system
f)	Odisha One	E&IT Department, Govt. of Odisha	To show the available balance of the beneficiary
g)	Odisha Birth & Death Registration System (OBDRS)	Health & Family Welfare Department	Registration of Birth and Death Event
h)	PFMS/ IFMS	Finance Department, Govt. of Odisha	To conduct frictionless payment with the empaneled hospitals
i)	Jana Sunani	E&IT Department, Govt. of Odisha	Redressal of Grievances

Sl#	Name of the Application	User Department	Purpose of Integration
j)	Mo Sarkar	E&IT Department, Govt. of Odisha	Feedback from Citizens/Hospitals
k)	Digital Signing Solution	E&IT Department, Govt. of Odisha	For DSC and e-Sign of records during approval process. (Signing Solution shall be provided by OCAC)
l)	SMS/ Email,	E&IT Department, Govt. of Odisha	To share alerts and notifications to the users
m)	WhatsApp	E&IT Department, Govt. of Odisha	
n)	Social Media (face book, Twitter)	E&IT Department, Govt. of Odisha	To capture the feedbacks from the users

2.7 Testing

- a) The new SI shall provide the testing strategy including Traceability Matrix, Test Cases and Conduct Testing of various components of the software developed / customized (e.g. including Unit Tests, System Integration Tests, Security Testing and Functional Acceptance Test).
- b) Details of the testing strategy and approach should be provided in the response.
- c) The new SI is responsible to identify and inform OCAC regarding testing requirements and impacts. The new SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined.
- d) The new SI must ensure deployment of necessary resources and tools during the testing phases and shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing.
- e) It is the ultimate responsibility of the new SI to ensure that the end product delivered, meets all the requirements specified in the document.
- f) The new SI shall take remedial action based on outcome of the tests.
- g) The new SI shall provide complete support to departmental officials or their representatives at the time of user acceptance testing.
- h) It would be the new SI's responsibility to ensure that all issues raised during UAT are closed and signed-off from respective authority.
- i) The new SI shall ensure that each module & features developed under this RFP is tested as per the latest version of the IEEE 730 (Software Quality Assurance Processes) standards and shall comply with GIGW guideline.

2.8 Third Party Audit

- a) The new SI needs to ensure that the solution is in compliance with the CERT-In Security Policy and Guidelines.
- b) The new SI shall appoint CERT-In empaneled auditor who shall be responsible for performing the security audit of the solution.
- c) The cost of audit & rectification of non-compliances shall be borne by the new SI.
- d) Carryout security audit before go-live of application and obtain the safe-to-host certification
- e) Carryout the periodic audit & certification as and when it is required as per the OSDC policy.
- f) The audit shall be performed at least on the below mentioned aspects.
 - Accessibility Testing
 - Application Security Audit
 - Vulnerability Testing
- g) The illustrative deliverables for this activity are mentioned below.

<i>Activity</i>	<i>Responsibility</i>
First Round Audit Report	Auditor
Rectified solution and submission of next round of audit	new SI
Next Round Audit Report	Auditor
If required, rectified solution & submission of next round of audit	New SI
Compliance Confirmation	Auditor

2.9 SSL Certification

The new SI shall carry out SSL certification.

- a) Secure connection between Client and Server through Secure protocol HTTPS
- b) Encryption of Data during transmission from server to browser and vice versa
- c) Encryption key assigned to it by Certification Authority (CA) in form of a Certificate.
- d) SSL Security in the application server

2.10 Training

- a) The new SI is required to undertake training on a train the trainer mode.
- b) Training would be done at State Headquarter in Bhubaneswar
- c) OCAC will facilitate the training space & related logistics
- d) The new SI shall set up the IT infra such as computer, network, LCD, etc as required

for providing the training in a successful manner.

- e) The schedule / training calendar and the training material for imparting training shall be developed by the new SI in consultation with OCAC, SHAS team and department officials. The new SI shall submit a hardcopy of the training material to OCAC before every training session.
- f) In case of modifications, either in the training plans or substitutions of the regular trainers, proper communication with OCAC and Participating Department need to be made.
- g) **If required, the new SI may conduct the training on virtual mode and related expenditure for licensing (fixed & recurring) shall be borne by the new SI.**

2.11 Online Help / Reference with Search Option

- a) It is also proposed that the training contents / user manuals be made available to users in downloadable (PDF) format so that the users may refer / download it for their own personal reference as and when needed.
- b) It is required that the downloadable training content should have proper indexing and internal references, mapped with key words, in order to allow any user to search and reach the desired content with the help of those key words.
- c) It is envisaged that any user will be able to search and read the directions / information for the right content. On entering the key words for search criteria, the system should pull out and display the links to the content as mapped.
- d) The system should support dynamic search facility i.e. as soon as the key words are changed; a new set of content links with page shall be displayed to the user.

2.12 Supply of tools and license

The new SI shall procure the database, middleware, Integration tool, Analytics, Data encryption & security license for this project in name of OCAC as per the specification and bill of quantity mentioned in this RFP and proposed by SI in its technical proposal as well.

2.13 Deployment & Configuration

- a) The new SI shall deploy the new application / portal over the hardware infrastructure provided by the OSDC / cloud.
- b) The new SI shall be responsible for the end-to-end management of hosting and deployment of the application.
- c) The new SI will be responsible for configuration, installation and hosting of the application in High Availability mode at OSDC / cloud.
- d) The new SI shall ensure deployment of the application as per the DR policy of OSDC

2.14 UAT & Go-Live

After completion of the development work for application, OCAC will conduct the technical reviews of development work performed by the new SI as UAT. The new SI shall be responsible for:

- a) Preparation and submission of test strategy, test cases and test results
- b) Demonstration of module-wise functionalities/ features before the OCAC in staging environment
- c) Support OCAC and its designated authority for conducting the testing and provide access of the systems as required by them.
- d) Rectification in the new application for any issues/ bugs/ and improvements/ Enhancements / up-gradations suggested Departments (if any) during the UAT without any additional cost.

2.15 Data Migration

During development of the BSKY2.0 application, the new SI needs to migrate data from the existing BSKY system to the proposed BSKY 2.0. The Data Migration to be performed by the new SI shall be preceded by an appropriate Data Migration Strategy & Methodology which is to be prepared by the new SI and approved by OCAC.

Data Migration should be carried out as per industry practice and all care must be taken to log in each error. The new SI should clearly define the data migration strategy in the proposal. The following activities will be carried out as part of the Data Migration:

- a) Define all the specifications that are needed to populate the data into the new system
- b) Prepare the Data cleaning and migration plan and submit to concern authority for approval.
- c) Prepare uniform codification of all data sets
- d) Identification, configuration or development of the data upload / download programs for the Data Migration
- e) Ensure minimum business downtime at the time of data cleaning and migration
- f) Ensure the accuracy and completeness of the migrated data
- g) Ensure migration of all data is completed by the time of Go Live
- h) Database of existing system would be migrated to the newly developed system
- i) The new SI will be expected to understand the data which has been captured and

devise a template so that meaningful information can be captured and entered into the new system

- j) This template should have basic sanity check to prevent entry of incorrect information. E.g. numerals should not be allowed in patient name etc.
- k) It is the ultimate responsibility of the new SI to ensure that all the data sets which are required for operationalization of the agreed user requirements are migrated.
- l) OCAC will provide the database of the existing system and new SI is to manage the data extraction, normalization & migration for the new system developed.

2.16 Infrastructure Support

- a) The solution is presently hosted in OSDC.
- b) Post award of contract, the new SI will be expected to detail hardware sizing. Based on sizing of the hardware by the new SI, the additional hardware (if required) will be arranged/procured separately by OCAC.
- c) The new SI shall carry out the installation, maintenance & support of all the supplied software(s) on the newly procured / existing hardware for development, quality and production environment.

This clause is related to the assessment of the gap infrastructure requirement which will include server, storage, security devices and related system software. Activities for this clause are as follows:

2.16.1 Implementing Software & Tools

- a) The new SI shall design, implement/customize the solution and shall install supplied tools and licenses as mentioned in the BOQ.
- b) The observations of the audit shall be addressed and same shall be tested and verified again before the go-live.

2.16.2 Business Continuity Planning

Currently, there is no DR or BCP to address any disruption in implementation of the system. However, in future, if it is decided to go for DR / BCP, then the new SI will suggest and support for an appropriate methodology in a cost effective manner for this purpose.

2.16.3 Documentation

- a) The new SI shall undertake preparation of documents including that of infrastructure solution design and architecture, configuration files of the infrastructures, user manuals, Standard Operating Procedures, Information Security Management procedures as per acceptable standards.

- b) The SI shall take sign-off on the deliverables (documents), including design documents, Standard Operating Procedures, Security Policy and Procedures from OCAC / OSDC Team and shall make necessary changes before submitting the final version of the documents.

2.17 Call Centre Operations

- a) Call center will be set-up to provide support to the beneficiaries and general public
- b) The existing 104 call center will be used to provide necessary call center supports to the patients, attendants and general public, which will be facilitated by OCAC / Health Department.
- c) Required training on the application software (BSKY2.0) to the Call Center executive will be provided by the new SI.
- d) The Call Center executive will provide following support to the stakeholders but not limited to;
- Attending user queries on scheme eligibility
 - Provide guidance on BSKY scheme availability
 - Provide information on card status/ balance on card etc.
 - Provide information on the list of hospitals empaneled district wise disease wise etc.

2.18 Technical Support Unit

The technical support unit at different location will be to be set-up and managed by the new SI.

2.18.1 State Level

The new SI shall setup a dedicated technical support unit equipped with experts and computing infrastructure to provide technical and functional support to the department/SHA users, hospital users, claim processed doctors and SNA doctors.

This unit shall be the first point of contact for the concerned stakeholders for resolving all application related incidents of service request. It aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service-quality and availability are maintained.

The new SI will set-up the above unit and operate in its premises within the Bhubaneswar Municipality Corporation area and OCAC has full rights to access the premises for its supervision as and when it is required. The above unit will function on 24X7 basis. All recurring and fixed cost will be borne by the new SI.

The deployed team shall perform following activities

- a) Attending user queries on application non functionalities issues
- b) Co-ordinate with software team for all types of issue management / redressal in relation to the application software, selection list, MIS reports, etc.
- c) Provide administrative support for creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support
- d) Furnish periodic report on number of issues received vis-a-vis resolved related to software
- e) Manage the framework and provide application rights
- f) Escalation of issues to backend software team
- g) Analyze feedbacks received from users
- h) Coordinate with the team to resolve user issue
- i) Provide support to users through phone calls/ email
- j) Troubleshooting through remote support for smooth functionality of the application
- k) Provide training / retraining to the users to use the application
- l) Resources of following skill will be deployed in the technical support unit

Designation	Qualification and experience
System Engineer	BE/ B.Tech/ MCA with minimum 3 years' of experience in software development and implementation work

2.18.2 Districts in Odisha

Health & Family Welfare Department is primarily intended to use the following service but will confirm through separate change order at the time of requirement. However, minimum contract period will be 12 months.

- a) The new SI shall deploy dedicated technical resources at different district of Odisha to provide support to the functionaries (dealing with BSKY matters) of the empaneled hospitals in that particular district.
- b) The technical resource shall report to the CDMO or any other officer decided by H & FW Department/SHAS.
- c) The technical resource shall be the first point of contact for all concerned stakeholders of that particular district.

- d) The technical person will be available physically in the CDMO office in all government working days.
- e) SHAS/OCAC reserves right to increase and decrease number of resources at the Districts. Payment shall be made on the basis of actual number of resources deployed.
- f) The SI should deploy the District level resources (District Coordinator) after getting confirmation from OCAC/SHAS.
- g) The technical person shall perform following activities
 - Attending user queries on application non functionalities issues
 - Provide support through phone calls / email, if not feasible to travel to that hospital.
 - Provide training / retraining for better use of the application
- h) Resource skill requirement

Designation	Qualification and experience
District Coordinator	Any Graduate with PGDCA having 3 years experience in IT Support with good interpersonal and communication skills

- i) All recurring and fixed cost related to IT will be borne by the new SI.
- j) Other logistics such as office space and related facilities will be provided by the health department.

2.18.3 Major Cities in India

Health & Family Welfare Department is primarily intended to use the following service but will confirm through separate change order at the time of requirement. However, minimum contract period for 12 months.

- a) The new SI shall deploy dedicated technical resources in major cities in India such as New Delhi, Kolkata, Mumbai, Chennai, Chandigarh, Surat, Pune, Bengaluru, Vizag, Lucknow, etc. to provide support to the functionaries (dealing with BSKY matters) of the empaneled hospitals in that particular city.
- b) The technical resource shall be the first point of contact for all empaneled hospitals of that particular city.
- c) The technical person would have physical presence (if required) in any empaneled hospital during local government working hours.
- d) The technical person shall perform following activities
 - Attending user queries on application non functionalities issues

- Provide support through phone calls / email, if not feasible to travel to that hospital.
 - Provide training / retraining for better use of the application
- e) SHAS/OCAC reserves right to increase and decrease number of resources at the Districts. Payment shall be made on the basis of actual number of resources deployed.
- f) The SI should deploy the major city level resources (City Coordinator) after getting confirmation from OCAC/SHAS.
- g) Resource skill requirement

Designation	Qualification and experience
City Coordinator	Any Graduate with PGDCA having 3 years experience in IT Support with good communication skills

- h) All recurring and fixed cost related to IT will be borne by the new SI.
- i) Local travel expenses (if any) will be reimbursed as per actual on production of supporting documents.

2.19 Operation & Maintenance

2.19.1 Application Support

Application support includes, but not limited to, production monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change management etc. The new SI shall keep the application software in good working order; perform changes and upgrades to applications as requested by the SHAS, Department of Health and Family Welfare and OCAC. Key activities to be performed by new SI in the application support phase are as follows:

- a) Enhancement of Analytical MIS report as per the requirement
- b) Database query report management on emergency
- c) Optimization of the already developed reports
- d) Tuning of transactions
- e) User & access management
- f) The new SI shall ensure compliance to SLAs as indicated in this RFP and any upgrades / major changes to the software shall be accordingly planned by SP ensuring the SLA requirements are met at no additional cost to department.

2.19.2 Software Maintenance

- a) The new SI shall provide support through Telephone / Email / Video Conferencing

/ Installation Visit as required as per the service window defined in the RFP

- b) The new SI shall address all the errors / bugs / gaps in the functionality in the solution implemented (vis-à-vis the FRS and SRS signed off) at no additional cost during the support phase.
- c) All patches and upgrades from OEMs (if any) shall be implemented by the new SI ensuring customization done in the solution as per the OCAC's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the new SI.
- d) Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the new SI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system.
- e) Tuning of products / applications, databases, third party software's and any other components provided as part of the solution software including reconfiguration of the system in the event of any hardware/ network failures/ if any hardware/ network components have to be replaced, shall be the responsibility of the new SI
- f) Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the new SI and periodically submitted to OCAC.

2.19.3 System/Infra Support

2.19.3.1 Database Administration

- a) Regular monitoring & management of all the applications installed / re-installed and databases hosted as and when it required for the project
- b) Installation & configurations the database
- c) Database administration, optimization and trouble Shooting
- d) Database & file back-up as per the policy of OSDC
- e) Perform Database, event & system log analysis

2.19.3.2 Server Administration

- a) Installation, integration and commissioning new servers applicable for this project
- b) Management & monitoring of servers such as Web, Application, Portal, Database & Middleware, etc. in cloud/OSDC
- c) Manage the DNS and Active directory activities
- d) Configuration of server parameters, operating systems administration and tuning
- e) Integration and user support on all supported servers, data storage systems, etc.

2.19.3.3 Security Administration

- a) Regular analysis of events and logs generated
- b) User ID and group management services

2.19.3.4 Backup & Restore Management

- a) Preparation of backup plan
- b) Backup of operating system, database and application as per SDC policy
- c) Monitoring and enhancement of the performance of scheduled backups

2.19.3.5 System / Network Administration

- a) Network configuration
- b) Patch update
- c) System Administration and Trouble Shooting
- d) Application & System Software Administration (including performance tuning)
- e) Application and database level performance tuning
- f) Co-ordination with OSDC Network Administration Team

2.20 Project Management

The envisioned project is a multi-disciplinary initiative. An effective project management plan and commitment to adhere to it is a mandatory requirement. The project plan should also include the resource, task and time plan for the entire duration of the project. The new SI shall employ best practices in project management methodology to ensure that the envisioned project components are developed and implemented within the defined time period. A copy of the project management plan shall be handed over to the department to keep track of the progress of the project

2.21 Guiding Principles

The proposed solution should adhere to the following principles.

2.21.1 Standards

- a) The system architecture should be based on industry standards and protocols
- b) The system will be centrally deployed and globally accessed
- c) The system shall be designed to be scalable and easily extensible
- d) The system should be flexible to cater to changing business, industry and compliance requirements (including reporting requirements in proper formats)

2.21.2 Application

- a) All applications must take into account appropriate security, performance, efficiency and maintainability issues.
- b) The ownership of the product licenses would be with OCAC.
- c) Upgrade to new releases should not become mandatory for the next three years from the date of installation.

2.21.3 Integration

The integrated solution design should include framework for integration of both internal and external applications and services using suitable architecture.

2.21.4 Data

- a) Data will be owned, shared, controlled and protected as a corporate asset of the OCAC.
- b) Data should only be accessed through application / interfaces to create, update and delete. There should not be any direct access to the data layer for users.

2.21.5 Data Security

- a) The new SI shall provide strategy to maintain data security at the application level
- b) The new SI shall provide strategy to maintain data security at the database level
- c) The new SI shall provide strategy to maintain data security at the messaging and middleware level
- d) The new SI shall provide security strategies when the applications are accessed from outside the network or accessing resources outside the network.
- e) The new SI shall provide strategies of encryption and security for external transaction with partner network and systems

2.22 Adherence to Standards

The system shall comply with relevant defined industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to its design, development, security, installation, and testing. The suggested architecture must be scalable and flexible for modular expansion. It should ensure ease of integration with software / applications developed using common industry standards since the solution may be linked and connected to other sources (websites, contents, portals, systems of other user departments etc.) as well as there may be loose/tight integration with backend system of other departments depending on individual service processes. The solution architecture should thus have provision to cater to the evolving requirements of the Department.

A reference list of the minimum industry standards which the system components should adhere to is mentioned below:

Component	Standards
Information Access / Transfer Protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open Standards
Portal Development	W3C Specifications
Document encryption	PKCS specification
Information Security	ISO 27001 certified System
Operation	ISO 9001 Certified
Service Management	ISO 20000 specifications or latest
Project Documentation	IEEE/ISO Specifications for documentation
Data Standards	All-important data entities should be in line with standards published by DeiTY.

2.23 Security, Integrity & Confidentiality

- a) **Web Services Security:** System shall comply to all the Web services including routing, management, publication, and discovery should be carried out in a secure manner. Those who are using the Web services should be able to utilize security services such as authentication, authorization, encryption and auditing. Encryption of data shall take place at client level itself. Application server shall provide SSL security.
- b) **Data Integrity and Confidentiality:** Data integrity techniques need to be deployed to ensure that information has not been altered, or modified during transmission without detection. Similarly, Data confidentiality features are also to be applied to ensure that the data is only accessible by the intended parties.
- c) **Transactions and Communications:** With respect to the Data Transactions and Communications, system needs to ensure that the business process are done properly and the flow of operations are executed in correct manner.
- d) **Non Repudiation Security:** The application shall have the Non-repudiation security services to protect a party to a transaction against false denial of the occurrence of that transaction by another party. End-to-End Integrity and Confidentiality of Messages The integrity and confidentiality of messages must be ensured even in the presence of intermediaries.
- e) **Database Controls:** The database controls for online transaction processing systems like access to database directly, access to database through application,

access to log files, access by the remote terminals, DBA controls, backup policy and backup procedures.

2.24 Change Management Team

The purpose of change management team is to ensure the agility in BSKY 2.0 to embrace the business changes in hassle free manner. The objective is to structure the change request management procedure so that the changes come frequently are implemented smoothly in faster way. It may be so required to customize the application to accommodate revise guidelines evolving time and again. Following are the indicative scope for change request.

- a) Application enhancement that will impact the business process and database
- b) Development of new forms and report
- c) New integrations
- d) Maintaining version of the code and artifacts through proper version management system for audit and future reference.
- e) Provide refresher training if needed for the change implemented in the system

Looking at the complexity and large user base of the project, it is expected to receive various queries and suggestions on the proposed BSKY 2.0 application. Hence department intends to reserve dedicated team to provide necessary changes in the application on a time and material basis. The department shall nominate a single point of contact who will coordinate with the team for the changes or suggestions received from end users.

Required software licenses, network, computing infrastructure, etc for creation of development environment, testing environment and staging environment will be the responsibility of the new SI. The above environments for the change management team would be set-up by SI in its premises within the Bhubaneswar Municipality Corporation area and OCAC would have full access rights to the premises for its supervision as and when it is required.

So a dedicated software team as per the following skill is required which can frequently deliver the tangible change in the form of new features and functionality.

SI#	Description	Qualification and Experience
a)	Team Lead	BE/B.Tech/MCA with minimum 10 years of experience in Team handling and project coordination
b)	Sr. Software Engineer	BE/B.Tech/MCA with minimum 5 years of experience in application development

Sl#	Description	Qualification and Experience
c)	Sr. Test Engineer	BE/B.Tech/MCA with minimum 5 years of experience in test plan preparation, test case review, test scenarios/condition preparation, test data preparation having ISTQB certification
d)	Application Security Expert	BE/ B.Tech/ MCA with minimum 6 years of experience in IT application security management having certification like CCNA/CISM etc.
e)	Database / System Administrator	Master Degree with minimum 7 years of relevant experience and OEM certification

During this time any change requests received from the department will be implemented by the aforesaid team in following manner

- a) Understanding change requests and analyzing impact of desired change on existing modules
- b) Revising the requirement specifications, design document prepared earlier including traceability matrices, test plan, test cases and other related technical artifacts to incorporate desired change
- c) Demonstrate the changes incorporated in the application as per the requirement shared by department.
- d) Redeploy upgraded version of the application onto the staging, training and production environment
- e) Closing the change-request-ticket after receiving note of satisfaction from the department

2.25 Exit Plan

- a) The selected firm will provide systematic exit plan and conduct proper knowledge transfer process to handover operations to OCAC technical team at least three months before project closure.
- b) IT resource persons of OCAC will work closely with resource persons of the new SI at test, staging and production environment during knowledge transfer phase.
- c) All knowledge transfer should be documented and possibly recorded.
- d) The SP will ensure capacity building of the IT resource persons of OCAC on maintenance of software and infrastructure.

2.26 Project Documentation

The new SI will share below list of documents to OCAC during the project contract period.

- a) Latest version of Source Code
- b) System Requirement Study Documents
- c) High Level Design (HLD) / Low Level Design (LLD) documents including
 - i) Application architecture documents
 - ii) ER diagrams and other data modelling documents
 - iii) Database design
 - iv) Application component design including component deployment views, control flows, etc.
 - v) Application flows and logic
- d) Test Plans and Reports
- e) Issue Logs
- f) User Manual
- g) Application Installation & Configuration Manual
- h) Report of Security Audit & Safe-to-Host Certificate
- i) Any other documents defined under Timeline & Tentative Deliverables
- j) All the above documentation should be done as per IEEE/ISO/CMM Standard

2.27 Expected Deployment of Personnel

- a) The bidders shall furnish resumes of key personnel to be engaged during software study, design, development, testing, UAT, implementation, operation & maintenance phase.
- b) The bidder shall submit a detailed work plan showcasing involvement of key resources in their technical proposal.
- c) The bidder shall engage the same personnel for the period of at least six months from date of commencement of project.
- d) The resources will work from the bidder's premises. However the resources should be available at client office for any meeting or discussions required by the client as per its convenient.
- e) The minimum criteria for key resources are as follows.

Competency Area	Minimum Educational Qualification and Experience
Program Manager	<ul style="list-style-type: none"> – B.E/B.Tech/MCA & MBA – Minimum 20 years’ experience of handling similar large projects in IT Sector. – Out of these, 10 years’ experience in handling state wide rollout project Certification: Prince2 or PMP
Project Manager	<ul style="list-style-type: none"> – BE/B.Tech/MCA – Minimum 12 years’ experience of handling similar large projects in IT Sector. – Out of these, 7 years in the field of software development and implementation. Out of these 7 years, 5 years’ experience in healthcare domain for any government department in India. – Certification: Prince2 or PMP
Tech Lead	<ul style="list-style-type: none"> – BE/B.TECH/MCA – Minimum 9 years’ experience in the field of software development and implementation. – Out of these 9 years, 4 years’ experience in healthcare domain for any government department in India.
Solution Architect	<ul style="list-style-type: none"> – B.E/B. Tech/MCA – Minimum 10 years of experience in the field of software design & development – Out of these 10 years, At least 5 years’ experience in large-scale software projects as a solution architect – Certification: TOGAF or relevant IT certification
Software Test Lead	<ul style="list-style-type: none"> – BE/ B.TECH/ MCA – Minimum 8 years’ experience in software testing. – Certification: ISTQB
Database Administrator	<ul style="list-style-type: none"> – B.TECH / MCA – Minimum 6 years’ experience in large scale software projects as DBA. – Certification: relevant OEM certification

2.28 Expected Project Timeline

2.28.1 Timeline for managing the existing BSKY application

Sl#	Milestone	Timeline
a)	Handover & Takeover process	Within 3-months from the effective date of contract

Sl#	Milestone	Timeline
b)	Maintenance of the existing BSKY application	3-Months from the date of handover and takeover process is completed

2.28.2 Timeline for the New BSKY 2.0 application

The BSKY2.0 will be implemented in two phases as per below table

Phase-I	Phase-II
<ul style="list-style-type: none"> – User & Master Management – Hospital Registration – Claim Management System – Self Service 	<ul style="list-style-type: none"> – Transaction Management System – Dashboard & MIS – Grievance Management – Mobile Application

Hence the timeline of the above phases are given below

Sl#	Milestone	Timeline
Modules / sub-modules under Phase-I		
a)	Completion of system requirement study (SRS) and submission of document	Within 1-month from the effective date of contract
b)	Completion of Design and Development of the application as per the approved SRS	Within 3-months from the effective date of contract
c)	Start of User Acceptance Test (UAT)	
d)	Security Audit by CERT-In empaneled auditor / agency	Within 1-month from the date acceptance of UAT
e)	Training and go-live of the application	Within 15-days from the receipt of security audit certificate
Modules / sub-modules under Phase-II		
f)	Completion of system requirement study (SRS) and submission of document	Within 4-months from the effective date of contract
g)	Completion of Design and Development of the application as per the approved SRS	Within 5-months from the effective date of contract
h)	Start of User Acceptance Test (UAT)	
i)	Security Audit by CERT-In empaneled auditor / agency	Within 1-month from the date acceptance of UAT

SI#	Milestone	Timeline
j)	Training and go-live of the application	Within 15-days from the receipt of security audit certificate
k)	Start of Application Maintenance and Support service of BSKY2.0	From the date of go-live of modules under Phase-II
l)	Start of technical support unit	From the day of taking over of existing BSKY application (i.e. start date of O & M of existing application by new SI)
m)	Deployment of dedicated change management team	From the date of go-live of modules under Phase-I
n)	Tools and Licenses (Database, Middleware, Analytics, Data encryption and security, etc)	Within 3-months from the effective date of contract

2.28.3 Timeline for IaaS and PaaS (Oracle ExaCC)

SI#	Project Activity / Scope of work	Deliverable	Timeline
a)	Completion of activity as mentioned under clause no. 3.11.1	Delivery of Hardware System as per BOM	120 days from the date of issuance of Purchase Order (OCAC will facilitated necessary Civil, Electrical, Network and other facilities within 15 days of issuing Purchase Order. Bidder has to deliver the Hardware within 105 days from the date of redlines of the infra.)
b)	Completion of installation as mentioned under clause no. 3.11.1	Successful installation report	60 days from the date of delivery
c)	GO-live of DB cloud Service	DB services activated from SDC	30 days from the date of successful installation.
d)	Provide Managed Services and Technical Support	Monthly Report	48 Months from the date of Go-Live

2.29 Service Level & Penalty

If the selected bidder fails to achieve the below scope of work within the corresponding Delivery Period and any extension thereof, unless such failure is due to

force majeure situation or due to OCAC's default, penalty shall be imposed by OCAC on the selected bidder.

2.29.1 New BSKY 2.0 Application

Sl#	Major Area	Parameter	Requirements	Penalty
a)	Development & Implementation	Major milestone during development and implementation as per project timeline.	As per project timeline	Rs. 500/- per day delay
b)	Response time for bug fixing	Time taken (after the request has been informed) to acknowledge problem	Within 24 hours from the time the bug is reported.	Rs. 100/- per hour delay
c)	Resolution Time (Only for Bug fixing)	Time taken by the service provider to fix the problem	Problems with severity within 48 hours from the time of reporting.	Rs. 500/- per hour delay
d)	Technical Support Unit	Start of service	As per project timeline	Rs. 200/- per day delay

2.29.2 IaaS and PaaS

Sl#	Project Activity / Scope of work	Timeline	Penalty
a)	Completion of activity as mentioned under clause no. 3.11.1	120 days from the effective date contract.	A penalty @ 0.1% per week on the component subject to maximum of 5% of the total contract value
b)	Completion of installation as mentioned under clause no. 3.11.1	60 days from the date of delivery	A penalty @ 0.1% per week on the component subject to maximum of 5% of the total contract value
c)	GO-live of DB cloud Service	30 days from the data of successful installation	A penalty @ 0.1% per week on the component subject to maximum of 5% of the total contract value
d)	Managed Services and Technical Support	Start of service	A penalty @ 0.1% per week on the component subject to

SI#	Project Activity / Scope of work	Timeline	Penalty
			maximum of 5% of the total contract value

2.29.3 Waiver of Penalty

If at any time during the Contract, the selected bidder should encounter conditions impeding timely performance of service, the selected bidder shall promptly notify to OCAC in writing of the fact of the delay and its likely duration along its cause(s). As soon as practicable after receipt of the selected bidder's notice, OCAC shall evaluate the situation and may at its discretion waive the penalty on the request of the selected bidder.

2.30 Bill of Material & Quantity

SI#	Category	Items	Qty
a)	Handover and takeover of the existing BSKY application	As per the scope mentioned in the clause 2.2.1 of this document.	Lump sum
b)	Application Maintenance and Support of the existing BSKY application	As per the scope mentioned in the clause 2.2.2 of this document.	6 Months
c)	Implementation of BSKY2.0 application	Study, design, development, security audit, training, go-live, documentations, etc as per requirement mentioned under clause no. 3 of this document.	Lump sum
d)	Application Maintenance and Support of the BSKY2.0 application	Application Support, Software Maintenance, System Support, etc mentioned under clause 2.19 of this document.	3-Years

Sl#	Category	Items	Qty												
e)	Technical Support Unit for department users, hospital users, claim processed doctors and SNA doctors	Helpdesk support 24X7 (round the clock) as per requirement mentioned under clause no. 2.18 of this document with flowing quantity <table border="1"> <thead> <tr> <th>Type of resources</th> <th>Qty</th> </tr> </thead> <tbody> <tr> <td>System Engineer</td> <td>3 persons each in 3 shifts = 3x3=9 Reliever = 2</td> </tr> <tr> <td>Total</td> <td>11 Resources</td> </tr> </tbody> </table>	Type of resources	Qty	System Engineer	3 persons each in 3 shifts = 3x3=9 Reliever = 2	Total	11 Resources	3 Years and 3 months						
Type of resources	Qty														
System Engineer	3 persons each in 3 shifts = 3x3=9 Reliever = 2														
Total	11 Resources														
f)	Technical Support Unit [District Level] for empaneled hospital inside Odisha	Technical support as per requirement mentioned under clause no. 2.18.2 of this document with flowing quantity	Minimum 12 Months												
g)	Technical Support Unit [Other Cities] for empaneled hospital inside Odisha	Technical support as per requirement mentioned under clause no. 2.18.3 of this document with flowing quantity	Minimum 12 Months												
h)	Change Management Team	As per the clause 2.24 of this document with following quantity <table border="1"> <thead> <tr> <th>Type of resources</th> <th>Qty</th> </tr> </thead> <tbody> <tr> <td>Team Lead</td> <td>1</td> </tr> <tr> <td>Sr. Software Developer</td> <td>3</td> </tr> <tr> <td>Sr. Test Engineer</td> <td>1</td> </tr> <tr> <td>Application Security Expert</td> <td>1</td> </tr> <tr> <td>Database / System Administrator</td> <td>1</td> </tr> </tbody> </table>	Type of resources	Qty	Team Lead	1	Sr. Software Developer	3	Sr. Test Engineer	1	Application Security Expert	1	Database / System Administrator	1	3-Years
Type of resources	Qty														
Team Lead	1														
Sr. Software Developer	3														
Sr. Test Engineer	1														
Application Security Expert	1														
Database / System Administrator	1														
i)	SSL certificate	As per the scope mentioned in clause 2.9	36 Months												
j)	Cyber Security Audit	As per the scope mentioned in clause 2.8	10 nos.												
k)	Analytical Tool	Supply of tools as per the scope mentioned in clause 3.10 of this document and quantity proposed by SI	License with 3 year support												
l)	Middleware Tool	Supply of tools as per the scope mentioned in clause 3.10 of this document and quantity proposed by SI	License with 3 year support												
m)	Integration Tool	Supply of tools as per the scope mentioned in clause 3.10 of this document and quantity proposed by SI	License with 3 year support												

Sl#	Category	Items	Qty
n)	Data encryption and security Tool	Supply of tools as per the scope mentioned in clause 3.10 of this document and quantity proposed by SI	License with 3 year support
o)	SMS	License and recurring expenses required as per the technical proposal of the SI. Tentatively 1 Crore SMS would be sent in different stages services during a year.	1 Crore SMS per Year
p)	Email	License and recurring expenses required as per the technical proposal of the SI. Tentatively 25 lakhs Email would be sent in different stages services during a year.	25 lakhs Email per Year
q)	WhatsApp	License and recurring expenses required as per the technical proposal of the SI. Tentatively 50 lakhs WhatsApp message would be sent in different stages services during a year.	50 lakhs WhatsApp per Year

2.31 Payment Terms

2.31.1 Management of existing BSKY application

Sl#	Milestone	Deliverables	Payment Terms
a)	Handover & Takeover process	Handover and Takeover document with self-declaration to this effect	100% of the quoted cost
b)	Maintenance of the existing BSKY application	Maintenance activity report	Quoted cost equally divided by duration (month)

2.31.2 Implementation of New BSKY 2.0 application

Sl#	Milestone	Deliverables	Payment Terms
Modules / sub-modules under Phase-I			
a)	Completion of system requirement study (SRS)	SRS document approve by OCAC/user department	20% of the quoted cost
b)	Completion of User Acceptance Test (UAT)	UAT Certificate by OCAC/user department	40% of the quoted cost

Sl#	Milestone	Deliverables	Payment Terms
c)	Training and go-live of the application	Go-live Certificate by OCAC/user department	20% of the quoted cost
Modules / sub-modules under Phase-II			
d)	Completion of system requirement study (SRS)	SRS document approve by OCAC/user department	20% of the quoted cost
e)	Completion of User Acceptance Test (UAT)	UAT Certificate by OCAC/user department	40% of the quoted cost
f)	Training and go-live of the application	Go-live Certificate by OCAC/user department	20% of the quoted cost
g)	Application Maintenance and Support service of BSKY2.0	Maintenance activity report	<ul style="list-style-type: none"> – Quoted cost equally divided by duration (<u>quarter</u>) – Balance 20% of Phase-I and Phase-II module equally divided by 4-quaetrs
h)	Technical Support Unit	Monthly activity report	Quoted cost equally divided by duration (<u>quarter</u>)
i)	Change Management Team	Quarterly activity report	Quoted cost equally divided by duration (<u>quarter</u>)

2.31.3 OEM License

Sl#	Milestone	Deliverables	Payment Terms
a)	Supply of tool and license with 1 st year Annual Technical Support	License in name of OCAC	100% of the quoted cost
b)	2 nd and 3 rd year Annual Technical Support of the supplied tools and license	Documentary evidence on support of renewal	100% of the yearly quoted cost at the beginning of respective year

2.31.4 IaaS and PaaS

Sl#	Project Activity / Scope of Work	Deliverables	Payable Amount
i)	Hardware Infrastructure (IaaS) including Compute, Storage and networking required to connect to the SDC Network.	Supply and Delivery of the Hardware device for IaaS Infrastructure at OCAC SDC.	Subscription for IAAS will be paid quarterly in advance for the period of the contract (4 years)

Sl#	Project Activity / Scope of Work	Deliverables	Payable Amount
	<i>*Bidder are requested to ensure they have the right understanding of the SDC and quote all required connectors, Cables, jumpers etc. OCAC will not be responsible for any supply in this regard</i>	<i>(OCAC will need to certify on the delivery)</i>	
ii)	PaaS subscription for Oracle Database Ent Edition.	Successful installation and commissioning of the PaaS Infrastructure <i>(OCAC will need to certify the successful integration with SDC)</i>	Subscription for PAAS will be paid quarterly in advance for the full duration of the contract (4years)
iii)	Installation cost of Hardware Infrastructure (IaaS) in SDC.	Successful Installation and commissioning of the IaaS Infrastructure mentioned in Sl.1. <i>(OCAC will need to certify the successful Installation)</i>	100% payment will be made on successful commissioning of the infrastructure.
iv)	Managed Services and Technical Support for 4 Years after go live	Activity report	Payment will be made on quarterly basis

2.31.5 Recurring Expenses

Expenses incurred for SMS, Email and WhatsApp would be reimbursed as per actual basis. So the SI will take prior approval from OCAC on the tentative requirement along with the estimate before purchase of these services.

2.31.6 General Conditions

- a) Payment schedule - Payments to the bidder/authorized partner, after successful completion of the target milestones (including specified project deliverables), would be made as under: -

- b) The supplier's/ selected bidder's request for payment shall be made to the purchaser in writing, accompanied by invoices describing, as appropriate, the goods delivered and related services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
- c) Due payments shall be made promptly by the purchaser, generally within thirty (30) days after submission of an invoice or request for payment by the supplier/ selected bidder/authorized partner, and the purchaser has accepted it.
- d) The currency or currencies in which payments shall be made to the supplier/ selected bidder under this Contract shall be Indian Rupees (INR) only.
- e) All remittance charges will be borne by the supplier/ selected bidder/authorized partner.
- f) In case of disputed items, the disputed amount shall be withheld and will be paid only after settlement of the dispute.
- g) Payment in case of those goods which need testing shall be made only when such tests have been carried out, test results received conforming to the prescribed specification.
- h) Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this bidding document, will be deducted from the payments for the respective milestones.
- i) Taxes, as applicable, will be deducted/ paid, as per the prevalent rules and regulations at the time of billing. Legitimate payment shall be made within 30 working days of the receipt of invoice along with supporting documents subject to penalties, if any.

3 Functional Requirements of BSKY 2.0

The objective of BSKY2.0 application is to provide health coverage to eligible Households of Odisha. The proposed application will have the following process and functionalities:

3.1 User & Master Management

This module will allow the admin user to manage users, groups, and roles defined for different users of the application. The admin user can define menu access rights for various users and user type. Different approval processes can be configurable as per the requirement. The system will allow users to upload files in different formats such as PDF, Word, Excel, HTML etc. System will capture information of adoption of audit trail mechanism. The user management module will have following functionalities:

SI#	Functional Requirement
A. User creation and Profiling	
FR01	The solution shall have the provision to create User
FR02	Provision to create type of user
FR03	The solution shall have facility to tag users with user types
FR04	Option for the administrator / individual users to update the user profile
B. Provide Application Access Rights	
FR01	Provision to define Menu hierarchy
FR02	The solution shall have facility to provide action rights to the users
FR03	The solution shall provide action rights like Add Right, View Right to the Users
FR04	Provision to copy access rights from one user to another user
C. Forgot and Change Password	
FR01	There shall be provision to change application login password by the user
FR02	Provision for the users to retrieve new password in case the user forgets his/her login credentials
D. Work flow Management	
FR01	The system shall have the provision for users to take action as per his/her assigned roles and rights.
FR02	Provision to view transaction in the application by the users.
FR03	The system shall have the facility to approve workflow for each process in the system
E. Master Management	
FR01	Provision to create various masters like Disease master, Scheme Master, Demographic master, Designation master
FR02	The system shall have the option to map the master fields in the subsequent module as per the requirement
F. Package Creation	
FR01	Provision to capture <u>Reserved Packages</u> information where treatment for minor ailments and diseases under National Health Programs are mostly reserved for government packages
FR02	Provision to avail treatment under <u>referral package</u> in registered private hospitals subject to the following conditions:

Sl#	Functional Requirement
	<ul style="list-style-type: none"> – Referral will be done if the particular package/ procedure cannot be provided by a Government facility in the district. – Cases will be referred if there is a long waiting time to undertake the procedure at a Government facility in the district. – Where there is an emergency cases which requires immediate referral. – Referral process under BSKY is decentralized up to Sub-Divisional Hospital level.
FR03	Provision to capture Open Packages for patient if the patient is found eligible under the package by the doctors who is also involved in treatment.
FR04	The system will have the provision to choose specialty from drop-down menu
FR05	Provision to choose package name/ package type
FR06	Provision to enter procedure name
FR07	Option to select package amount against disease
FR08	Provision to configure package by uploading mandatory and optional document at the time of claim process.

3.2 Hospital Registration

This module will help private hospitals to get empaneled for providing treatment to BSKY card holders under BSKY scheme. The Solution will have provision for the hospitals to register itself through the system. The empanelment will be valid for a period of 1 year. The solution should have following provisions for registration of hospitals:

Sl#	Functional Requirement
A. Hospital Empanelment	
FR01	Provision to fill Application form for empanelment / renewal / upgradation
FR02	Provision to capture hospital infrastructure details and other details
FR03	Provision to update hospital treatment status in the system
FR04	Provision to provide clarifications as sought by SHAS
FR05	Provision to check status of the application
B. Approval of Hospital Empanelment	
FR01	The system will have the provision to capture the details during the field visit by using mobile application by the official

SI#	Functional Requirement
FR02	Provision to verify Bank account
FR03	Provision to set the category of the hospital based on the field level verification
FR04	Provision to approve or reject empanelment by concerned stakeholder
C. CPD/SNA Doctor Registration	
FR01	The system will have the option to select/fill own hospital
FR02	Provision to enter specialization/super-specialization, experience, affiliation
FR03	Provision to edit the profile
FR04	Provision to approve by department authority after modification

3.3 Transaction Management System

SI#	Functional Requirement
A. Card Verification	
FR01	Provision to verify Fingerprint of beneficiary against data from smart card
FR02	Provision to verify Amount remaining in BSKY card
FR03	Provision to verify the eligibility of the patient through documentary evidence in case the name is not found in the database
FR04	Provision to check if beneficiary has already received treatment under the scheme by checking the card number
FR05	Provision to check the beneficiary eligibility as per business rules
B. Beneficiary Admission	
FR01	Provision to enter the NFSA/ SFSS / BSKY Smart Card Details in the Transaction Management System
FR02	Provision to display the members of card
FR03	Provision to select patient name from list of members name
FR04	Provision to authenticate the patient through IRIS/POS/OTP
FR05	Provision to select the patient as admitted
C. Case Transfer	
FR01	Provision to transfer the case to other Network/empaneled hospital.
FR02	Option to capture the date of transfer

SI#	Functional Requirement
FR03	Provision to capture following information like Address of hospital, Details of patient, Details of the attending doctor
D. Package Selection	
FR01	Provision to choose package as per treatment required
FR02	Provision to change/modify treatment package
FR03	Provision to Block multiple packages against one patient
E. Package Modification	
FR01	Provision to add packages during the course of treatment
FR02	Provision to modify package section
F. Pre-Authorization	
i) Hospital Request	
FR01	Provision to send Pre-Authorization request with MDR to SNA Doctor
FR02	Provision to fill patient details in the form, and upload necessary documents
FR03	Provision to submit document as per query received for more documents
FR04	The system will have the facility to block the package for patient treatment in case pre-authorization request is not verified within 24 Hrs / within 48 Hrs for Unspecified Package
ii) Pre-Authorization Verification	
FR01	Provision to check Pre-authorization and MDR
FR02	Provision to ask for more documents/send queries
FR03	The system will have facility to verify submitted documents
FR04	Provision to capture the time taken by the SNA doctor to attend a Pre-Authorization request
FR05	The system will have the option to approve/reject the pre-Authorization
G. Discharge	
FR01	Provision to update confirm status as “Discharged”
FR02	Option to discharge the patient by capturing biometric authentication along with upload facility for limited documents
FR03	Provision to enter a particular consultation date or regular interval checks in case further regular interval checks is required

3.4 Claim Management System

SI#	Functional Requirement
A. Claim Request	
FR01	Provision for Hospitals to request claim
FR02	Provision to provide details of the patients
FR03	Facility to upload Discharge document and other related documents
B. Claim Assign	
FR01	Provision for Auto Assigning of Claim to the stakeholders as per business rule
FR02	Option to auto assign Unprocessed claims to SNA doctors
FR03	The system will have the facility for Claim Transfer to another CPD in case of non-attended by assigned CPD within 72 Hours.
C. Claim Management	
i) by Claim Processing Doctors	
FR01	Provision for CPD to verify the received claims
FR02	The system will have option to Approve/ Reject on the Claims
FR03	Provision to capture the time taken by the CPD to attend a claim request
FR04	Provision for Sending queries to respective hospitals against Claim by annotating the queried page
FR05	Provision to Forward the Claims to SNA Doctors
FR06	Provision to capture CPD doctors login and log out time
FR07	Provision to anonymous identifiable details of a patient
FR08	Provision for System-based triggers to flag the suspicious claims,
FR09	Provision for System-based allocation of claims for review of flagged claims
ii) by SNA Doctors	
FR01	Provision for audit more than 10% of approved claim
FR02	Provision to audit 100% rejected and unprocessed claims
FR03	Option to Approve/ Reject on the Claims
FR04	Provision to capture the time taken by the SNA doctor to attend a claim request
FR05	Provision for Sending queries to respective hospitals against Claim by annotating the queried page
FR06	Provision to submit the approved claims for disbursement

SI#	Functional Requirement
FR07	Provision to capture SNA doctors login and log out time
D. Claim Disbursement	
FR01	Provision to generate csv file in the system
FR02	Option to apply maker/ checker/ approver policy for the claim disbursement

3.5 Development of Mobile Application

Provision to develop mobile application for both TMS and CMS module

SI#	Functional Requirement
FR01	Provision to capture hospital information during field visit
FR02	The system shall have provision for the field officers to capture photo with geo locations of the hospitals with necessary infrastructure availability status
FR03	Provision to conduct field inspection by field level user for rejected/unprocessed claims
FR04	Provision to develop the application in both Android and IOS platform
FR05	Provision for the doctors to view the claims and related documents through mobile app and take decision on the mobile app itself
FR06	The system will have option to view reports through mobile app
FR07	The system will have option to capture video feedback from the BSKY users through mobile app

3.6 Dashboard & MIS

The system should have a dashboard where various data visualization will be provided. Following are the few functionalities that should be present in the system:

SI#	Functional Requirement
FR01	Provision to generate turnaround time wise report, hospital wise report, district wise report
FR02	Provision for Map view reports on Hospitals empaneled
FR03	Provision for identification of suspects
FR04	Provision to view number of patients admitted like overall (Outpatient and Inpatient), Hospital wise, Procedure wise, Specialty wise
FR05	Option to display claim related information like <ul style="list-style-type: none"> – Flagged claims

SI#	Functional Requirement
	<ul style="list-style-type: none"> – Claim pending at doctors – Claim request vs Claim disbursement
FR06	Provision to generate various MIS reports such as <ul style="list-style-type: none"> – Overall summary of claim status – Daily summary of flagged claims – Allocation / selection of pre-authorizations, – Patient discharged without completion of treatment – Repeated admission for different procedures in same/ different hospitals – Discharge at odd hours of the night – Details of operator in one hospitals

3.7 Grievance Management

This module should manage all functions required to automate the grievance / complaint management lifecycle for various users/stakeholders. High-level features is outlined below;

SI#	Functional Requirement
FR01	Provision to raise tickets against each grievance by internal stakeholder
FR02	Provision to set priority of the ticket by internal stakeholders
FR03	Alerts and notification on the number of grievance generated, with flagging of type of grievance
FR04	Option to implement workflow mechanism for grievance address and resolution
FR05	Post resolution, option to close ticket by providing remarks against the grievance
FR06	Option to record turnaround time of grievance lodge to grievance resolved

3.8 Self Service

Following provisions shall be available in the solution:

SI#	Functional Requirement
A. Hospital	
FR01	Provision to check claim status
FR02	Option to check pre-authorization status
B. Beneficiaries	

SI#	Functional Requirement
FR01	Provision to check card amount
FR02	Provision to check the status of the claim
FR03	Provision to check status through Chat bot

3.9 General Features

3.9.1 Web Design Considerations

The Solution should be able to support all common browsers (like Internet explorer, Mozilla, Chrome, Safari etc). The new SI shall strictly follow Responsive Web Design (RWD) approach for developing user interfaces. At least labels used in the forms, reports etc. in the application shall be bilingual and be available in English and Odia language.

3.9.2 SMS and Email Facility

Proposed Solution should issue SMS alerts to the respective users for time bound actions and escalation mechanisms for non-attended activities. The new SI will integrate the relevant modules with messaging gateway provided by Health & Family Welfare Department, Government of Odisha for inbound or outbound SMS for different functionalities.

3.9.3 Data Export and Import Facility

This facility in the proposed solution enables users to download any report in MS Office and Open Office, CSV, PDF, XML formats. Similarly, the system should also allow the user to upload data from a MS-Excel, CSV, and XML wherever required.

3.10 Use of Emerging Technology

3.10.1 Analytics and Reports

The system shall have provisioned to generate various analytical report by using the proposed solution. This will help the departmental officials to take necessary actions as and when it is required. The reports should be displayed both in Tabular as well as graphical manner which will help the higher official to take action. Following are some

- a) Usage of Single card for single patient for consecutive years
- b) Usage of single card for multiple patient for consecutive years
- c) Card utilization more than 70% for consecutive years
- d) Age group Vs Disease
- e) Hospital applied for more than 5 lakhs limit frequently

- f) Maximum Pre authentication request against hospitals
- g) Provision to capture average time spent by the doctor on attending a claim request, pre- Auth request.
- h) Image Analysis for both pretreatment and post treatment

The proposed OEM tool shall cater to the below functionalities

SI#	Functional Requirements
FR01	There is a need for a robust enterprise grade business intelligence and analytics platform that can provide timely insights to users across an enterprise at a low overall total cost of ownership at any scale.
FR02	The solution should provide easy-to-use ad hoc query and analysis.
FR03	The solution should provide Self-service data visualization capabilities along with augmented analytics. Users should be able to drill, pivot, and filter their data directly on a dashboard, while a rich set of prompts and powerful right-click interactions open up even more advanced analysis capabilities. Users should be able to see information filtered and personalized based on their identity, function, or role processed via predefined security rules. Alerts, guided navigation links, and actions should be present to accelerate exception-based discovery of insight.
FR04	There should be capability to generate Pixel perfect enterprise reporting.
FR05	There should be a provision for providing powerful geospatial mapping and visualization as needed.
FR06	The solution should provide capability to get insights accessible to anyone, anytime, and anywhere with mobile business intelligence.
FR07	Users should be able to export data to various MS Office formats or add content to a list of favorites for quick access with one click access.
FR08	The solution should provide deeper insights by embedding machine learning and AI into every aspect of the analytics process. The user experience should be simplified with modern conversation-style analytics powered by natural language processing.
FR09	Users should be able to analyze from scratch or modify existing projects in dashboard pages. To free business users from data structure complexity, the solution should offer a logical view of metrics, hierarchies, and calculations expressed as understandable concepts. Business users should be able to combine data from multiple enterprise information sources without any understanding of physical data storage.
FR10	There should be robust Enterprise reporting capability that allows the creation of highly formatted templates, reports, and documents such as

SI#	Functional Requirements
	flash reports, checks, and more. It should be scalable and available for complex and distributed environments, and supports a vast number of data sources, including relational, multidimensional, web service, XML, and more. Users should be able to quickly and seamlessly transfer their data, layout, and format of a dashboard or analysis to an output or data export file.
FR11	The Analytics platform should provide a powerful, near-real-time, multistep alert engine that can trigger workflows based on business events and notify stakeholders via their preferred medium and channel.

3.10.2 Middleware Tool

As per the technical proposal of the bidder.

3.10.3 Integration Tool

Provision to use integration tool which shall act as a middleware and all data exchange shall be routed through the tool. The proposed integration tool should perform message routing, convert communication protocols and potentially manage the composition of multiple Requests. The tool should make integrations and transformations available as a service interface. Following activities shall be carried out by the integration tool

- a) Service management
- b) Application/Data Integration
- c) Data Transformation
- d) Data exchange
- e) Auditing
- f) Testing

The proposed tool shall cater to the following functional requirement

SI#	Requirements
FR01	There is a requirement for a robust enterprise grade integration solution that delivers faster time to integration, increased productivity and lower TCO.
FR02	The integration platform should be based on a comprehensive, standards-based software suite to build, deploy and manage integration following the concepts of service-oriented architecture (SOA).

SI#	Requirements
FR03	It should provide readily available adapters for virtually any scenario (REST, SOAP, File, Database, all leading applications, Mainframe etc.) thus saving time and effort and improving developer productivity manifold.
FR04	The integration platform should be scalable enough to support millions of critical transactions.
FR05	The solution should simplify integration and improve time-to-market for new business services by replacing complex point-to-point integrations with a single service virtualization connection.
FR06	It should provide simple, code-free, configuration-based integration and support rapid mobile enablement of smartphones and tablets.
FR07	The solution should provide embedded access to service result caching to eliminate latency for data oriented services.
FR08	The solution should provide automated SOA governance synchronization.
FR09	The solution should provide intelligent content and identity-based routing along with dynamic message transformation and streaming .
FR10	The integration solution should have built-in monitoring, management, and QoS.
FR11	The solution should provide optimized, pluggable, policy-driven transport and message security.
FR12	The solution should be compliant with WSRM and WS-Security standards.
FR13	The solution should provide extreme performance and unlimited scalability.
FR14	The solution should also provide built-in human workflow capabilities to allow for people to be included for approvals and reviews and also for exception management, or performing activities required to advance a given business process.
FR15	There should be capability to invoke notifications (such as email, instant messaging (IM), or short message service (SMS)) from Human Workflow to alert users of changes to the state of a task.
FR16	The human workflow capability should at least include the following features: <ul style="list-style-type: none"> – Human interactions with processes, including assignment and routing of tasks to the correct users or groups – Deadlines, escalations, notifications, and other features required for ensuring the timely performance of a task (human activity)

SI#	Requirements
	<ul style="list-style-type: none"> – Presentation of tasks to end users through a variety of mechanisms, including a work list application – Organization, filtering, prioritization, and other features required for end users to productively perform their tasks – Reports, reassignments, load balancing, and other features required by supervisors and business owners to manage the performance of tasks
FR17	The overall solution should not only include Service Bus and Workflow capabilities but also other capabilities such as Process Manager, Business Rules, Business Activity Monitoring and Event Processing all within the same integrated platform to cater to any current as well as future requirements (all available from the single OEM).
FR18	The application server should be enterprise grade and provide standards based APIs and tooling for application innovation on a proven mission critical runtime.
FR19	The application server should provide flexible deployment options including physical systems, VMs or cloud native Kubernetes environments.
FR20	The application server should provide clustering for high performance and high availability and also dynamic Clusters for elastic scaling.
FR21	The application server should support multiple runtimes such as Java EE 8, Java SE 8 and 11 and GraalVM EE Support.
FR22	There should be support for all popular IDEs along with CI/CD, testing, monitoring, and diagnostic tools for application development and management.
FR23	The application server should have inbuilt support for enterprise grade in-memory data grid for maximum scalability and performance.
FR24	Application server should provide enterprise support for micro-services based modern application development including the core micro-services framework along with tooling such as for containerization, orchestration, logging, monitoring etc. It should also provide out of the box operators to manage such a landscape.
FR25	The application server should provide enterprise scalability and clustering with features such as Session failover, whole server migration and automatic service migration for messaging and transaction services, and rolling upgrades. It should have providing for Automated, rules-based elastic scaling of dynamic clusters to automatically adapt to changing application requirements.

SI#	Requirements
FR26	The application server should enable users to record JVM events in an in-memory buffer that can be persisted for post-incident analysis.
FR27	Application server should provide native integration with underlying database for maximum performance, scalability and load balancing capabilities.
FR28	The application server should be certified to run on Docker and CRI-O containers and provide tools for the creation of the Kubernetes resources as well as simplifying lifecycle management operations such as starting, stopping and patching servers, and deploying and redeploying applications.

3.10.4 Data Encryption and Security Tool

As the proposed BSKY 2.0 application caters to the critical information of citizen, hence department envisages to use latest tools and technologies to ensure the data are kept in encrypted format in secured manner. Bidders are required to propose Encryption/ security Tool to cater following requirements.

3.10.4.1 File and Database level Encryption

The solution should facilitate segregation of duties" and access on a role and rights basis. It shall limit access to sensitive data. This security mechanism should be designed to meet compliance regulations determined by the government as well as globally practice industry standards. The proposed tool shall comply with below functional requirement.

SI#	Requirements
FR01	The change of the infrastructure environment should be minimized
FR02	The solution must be capable of being installed without application modification <ul style="list-style-type: none"> - No DB schema changes (view, index) - No business application changes
FR03	The solution should support various kinds of OS: Unix, Linux, Windows
FR04	The solution should support various kinds of data types <ul style="list-style-type: none"> - Unstructured data encryption such as WAS log file, backup file, configuration file, image, recording file - DBMS data store encryption
FR05	The solution should support various kind of data format <ul style="list-style-type: none"> - Large amounts of data - No impact on DB column type and data format (CHAR, INT)

SI#	Requirements
	<ul style="list-style-type: none"> - No impact on DB data format and constraint (PK, FK, NULL) - No increase of data size after encryption
FR06	<p>The solution should have the scalability of enterprise environment</p> <ul style="list-style-type: none"> - Big data environment - Cloud environment
FR07	<p>The solution should possess compatibility of current enterprise environment</p> <ul style="list-style-type: none"> - Transparent data access via application - Compatibility with backup and replication solutions
FR08	Performance degradation should be minimized
FR09	The solution should have certification and certified encryption algorithms
FR10	<p>The solution should support key management</p> <ul style="list-style-type: none"> - Full lifecycle of cryptographic keys management such as key generation, access, renewal, destruction should be provided by dedicated key management server and security should be ensured. - The encryption key must be securely protected on a separate server limiting access to the keys
FR11	<p>The solution should support audit and access control</p> <ul style="list-style-type: none"> - Access control on unauthorized user access to data - Audit log and report

3.10.4.2 Data Protection for Database

Data Protection solution for databases should provide automated sensitive data discovery and classification, real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data. It should protect against unauthorized data access by learning regular user access patterns. It should also have provision for generating real-time alerts on suspicious activities. It should dynamically block access or quarantine user IDs to protect against internal and external threats and also help streamline and automate compliance workflows. The product should be built on a scalable architecture that provides full visibility on data activity across all major databases. The proposed tool shall comply with following functional requirement.

SI#	Requirements
FR01	The solution should support integration with the critical databases such as DB2, Oracle, MS-SQL etc.
FR02	The solution should support integration with the Big Data platforms such as Horton Works, Data warehouse such as Exadata etc.

SI#	Requirements
FR03	The solution should offer automatic discovery of databases.
FR04	The solution should provide sensitive data discovery options together with predefined data classification rules for various sensitive data types including PCI data, PII data and offers the ability for customization
FR05	The solution should support user entitlement reviews on database accounts
FR06	The solution should implement blocking <ul style="list-style-type: none"> – For blocking the solution should be using an agent. – Solution should not be deployed in-line mode for blocking.
FR07	The solution should use agent-based architecture. <ul style="list-style-type: none"> – The solution agent should perform monitoring, blocking, redaction without any changes on the Database, network configuration & access mechanism.
FR08	The solution should not require any logging to be enabled at the database level. It should capture full SQL activities without enabling any database level logging.
FR09	The solution must monitor privileged user access or local SQL activity that doesnot cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes
FR10	The solution should have the ability to monitor data that is passed through encrypted transmissions such as oracle ASO
FR11	The solution should include specialized threat detection analytics that scan and analyze audited data to detect symptoms that may indicate malicious stored procedure
FR12	The solution should help in identifying abnormal server and user behavior and providing early detection of possible attacks using outliers. <ul style="list-style-type: none"> – For example, User activity that is identified as a suspected outlier includes: <ul style="list-style-type: none"> – User accessing a table for the first time – User selecting specific data in a table that he has never selected before – Exceptional volume of errors. – Activity that itself is not unusual, but its volume is unusual – Activity that itself is not unusual, but the time of activity is unusual. For example, a DBA is accessing a table more frequently than in the past. This could indicate that the DBA
FR13	The solution should support setting up of compliance monitoring. It should have out of box accelerators for PCI/DSS, Data Privacy.

SI#	Requirements
FR14	The solution should have multiple pre-configured policies & reports. Reports should address regulatory compliance such as SOX, PCI DSS, Data Privacy Law, GDPR etc.
FR15	The solution should have easy drag & drop option to customize report without developing or require lot of customization/changes from scratch.
FR16	Reports should be exportable via both PDF and Excel
FR17	All reports generated via the solution should be stored in a secure manner and all alterations to the report generation and to the reports themselves should be auditable
FR18	The solution should provide optimum utilization of resources by using Load balancing between servers. The solution should support Enterprise load balancing
FR19	The solution should support dynamic redaction for privileged user thus certain fields such as Aadhaar number, credit card number could be easily hidden from the privileged DBA"s.
FR20	The solution should use internal DB to store the Logs.
FR21	The solution should support normalization on the collected audit data thus if a same event occurs in short duration it should increase the count of event rather than creating a new event/log.
FR22	The solution should provide incident management module which will help business- user with workflow automation for tracking and resolving the database security incidents.
FR23	The solution should provide option of filtering option that only specific violation should be sent to SIEM.
FR24	The solution should have Vulnerability Assessment module which can discover unpatched vulnerabilities, default credentials, database default configurations/ misconfiguration.
FR25	The solution Vulnerability reports could be imported on a SIEM solution for providing a centralized vulnerability platform.
FR26	The solution should support integration with SIEM solution.
FR27	Solution must be able to prevent unauthorized activity based on command, table, database, IP, Application/OS/Database user name, time-based etc.
FR28	Proposed solution must be deployed without any network architecture change and down-time.

SI#	Requirements
FR29	Agent should not perform any processing such as normalization of activities. Solution should utilize less than 5% of operating system CPU utilization.
FR30	Solution must have temper-proof log storage capability
FR31	Solution should have flexible policy definition on the basis of who are the users, what they are accessing database/table, time of the day, from where they are accessing & how the user is accessing.
FR32	Policy action implementation should be defined.
FR33	Solution should capture SQL errors as well.
FR34	Solution must be capable to scale across multiple location with centralized management
FR35	Solution should be capable to discover database on the network, find and classify sensitive objects in databases.
FR36	Solution should be capable to detect default configurations, vulnerabilities on database without any changes/additional hardware in proposed solution.
FR37	Solution must support filtering/hiding of the bind variables of all the SQL activities captured.
FR38	The solution must identify down to the user level who is accessing which table & what SQL activity is performed by the database user
FR39	The solution should provide means to profile data activity behavior together with tools to filter noise or known false positives
FR40	Solution must be capable to monitor all type of user activity. This users can be local host, remote, database administrator, application user etc. and allow to configure to prevent specific command/user/table access
FR41	Solution support individual user access auditing for packaged applications, like SAP, PeopleSoft, Siebel
FR42	Audit records should contain all information required for understanding of the event including: Source and destination IP, DB and OS user name, source application, number of affected rows, and database instance name
FR43	The solution should not store sensitive data in logs generated by the application (e.g. passwords)
FR44	Logs and audit-trail generated by the solution should not be editable by users and should be read-only
FR45	The solution should provide an internal workflow capability that allows users to raise issues and assign them to other users
FR46	Alerting should be available via email, SNMP and Syslog

SI#	Requirements
FR47	Solution should be capable to integrate with third-party ticketing systems
FR48	Solution should proactively alert the administrators for any type of activity necessary including Syslog, SNMP, emails, and pagers, or custom classes for distribution of alerts
FR49	Solution must support role based access and integration with enterprise directories and RADIUS
FR50	Solution must be able to provide reports about database activity information including who logged in, DB user, application user, OS user, from where, how, etc.
FR51	Solution must be able to monitor and log database traffic that is encrypted with SSL or IPsec.
FR52	Solution must be able to capture complete DML, DDL statements and allow preventing unauthorized connection irrespective type of connection medium and user.
FR53	The solution should detect excessive, unnecessary, unauthorized, suspicious or high risk activity in real-time for both internal and external users including privileged users.
FR54	The solution should provide granular policy management by separate audit and security policies be created and managed at different granularity levels
FR55	Solution should support to create whitelist or exceptions list to ignore monitoring certain items (e.g., ignore a column that has zip codes only). Solution set granular policies down to such levels as table, column, specific application, specific type of database, specific user ID, specific IP address, etc.
FR56	The solution should be able to block excessive, unnecessary, unauthorized, suspicious or high risk activity in real-time for privileged users
FR57	The solution should audit accesses with elevated privileges, such as an administrator or system administrator account
FR58	Solution must support prevention time based policy. Such as time of day/week.
FR59	Solution must be able to perform content scanning for regular expression and patterns.
FR60	Solution must be scalable in distributed environment with centralized console.
FR61	Solution should support integration with LDAP

SI#	Requirements
FR62	Solution must have web based interface.
FR63	Solution must provide a Command-Line-Interface (CLI) for scripting/automation purposes
FR64	The solution should support integration with LDAP (AD)
FR65	The solution should provide database change management workflow enforcing separation of duties and traceability of changes

3.10.4.3 Vulnerability Assessment

Vulnerability Assessment solution shall enable the facility of scanning data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggest remedial actions. The solution shall identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports shall be provided along with suggestions to address all vulnerabilities. It shall detect behavioral vulnerabilities such as account sharing, excessive administrative logins and unusual after-hours activity. The solution should also have capabilities to identify threats and security gaps in databases that could be exploited by hackers.

The proposed tool shall cover following functional requirement

SI#	Functional Requirements-general
FR01	The proposed solution should provide easy & fast deployment. It should be available as a pre-deployed virtual appliance which could be deployed on hypervisor like VMware
FR02	The proposed solution Licensing should be based on Active Database Servercount
FR03	The proposed solution should not have extra licensing cost for UAT/ Development instances.
FR04	The proposed solution should have a product roadmap.
FR05	The proposed solution should integrate with all type of known databases in the organization

3.11 Requirement of IaaS and PaaS

Supply and installation of ORACLE ExaCC (detailed mentioned here under) and provide technical support. OCAC will provide ORACLE Database License along with other software mentioned here under the subsequent clause.

3.11.1 Supply and Installation of Hardware Infra

- a) Supply items as per the details provided in the Bill of Material & Technical Specifications.
- b) Supply of Hardware System as per the details provided in the Bill of Material & Technical Specifications on a Subscription model.
- c) Supply all required Cables, Connectors, for network as well as power connection to seamlessly integrate with the SDC Infra. In this regard, Bidders are requested to have a detailed understanding of the required components of the SDC setup, in consultation with OCAC.
- d) Install the items at the Odisha State Data Center, Bhubaneswar and obtain delivery & installation challan / certificates from respective nodal / designated officer.
- e) The bidder shall work with the OEM in a synchronized manner during the phases of delivery & installation of the infrastructure.
- f) The bidder shall provide Networking Solution architecture for Prod & Non-Prod for the supplied items.
- g) Understand the team's role and responsibilities to manage & design / update the compartments & policies.
- h) Create & setup of base services such as, Compartments, Administrative Users & Groups, Subnets, Security Lists, Routing Tables, Rules, Policies, etc.
- i) IPsec VPN Provisioning.
- j) Provision of the database consolidation platform with required shape & storage as per our requirement.
- k) Configure Auto Backup with required retention.
- l) Migration of existing databases to the database consolidation platform.
- m) Take prior approval from OCAC regarding the feasible downtime of the existing database for migration activities
- n) Suggesting necessary changes in the application tier so that the applications can communicate with the databases in the database consolidation platform.

3.11.2 Managed Services & Technical Support

Bidder shall provide technical support **(24X7)** basis for configuration, monitoring, patch update and optimization of configurable parameters in Oracle database. The scope of technical support are:-

- a) Tuning of the server environment.
- b) Strategic analysis and planning for database and infra
- c) Architecture consulting.

- d) Provide helpdesk/point of contact for technical support.
- e) Manage the VMs and instances
- f) 24x7 fault, performance and app monitoring
- g) Technical Assistance for the database management activities
- h) Incident management (if any)
- i) Cloud Migration advisory
- j) SOC, audit and compliance support (if any)

3.11.3 Bill of Material and Technical Specifications

Our objective is to have a database consolidation platform in a true subscription based consumption model which shall be designed to optimally run transactional & analytical database workloads together with a scale-out architecture. Our vision is to create modern applications with any type of data, development style & workload while automatically benefiting from high performance, consistent security models & mission-critical capabilities. We also want our databases are secured behind our data center firewalls to help meet our data residency, security & governance requirements. In comparison to our current database systems we want the offered database consolidation platform to deliver more database IOPS, higher analytics throughput & less SQL I/O latency. We also want to accelerate analytics & in-database machine learning applications by processing low-level SQL queries, analytics & machine learning algorithms in the database consolidation platform with high scan throughput of up to 500 GB/sec.

Sl#	Category	Functional Requirements	Compl ied (Y/N)	Reference
a)	Solution Type	The solution shall deliver the highest performing converged platform to run database as a service in a true subscription based burstable consumption model. All the hardware components in the offered solution shall be from the same OEM for the best integration & management. Mix & Match of Multi-OEM products in the offered solution is not permissible.		
b)	Installation	The system/s offered in the solution shall be deployed by a specialized OEM engineer only. The engineer shall come onsite, deploy the system/s in our data		

Sl#	Category	Functional Requirements	Complied (Y/N)	Reference
		center, connect the system/s to our network & configure the system/s to communicate with the Control Plane. Before handing over the system/s the OEM shall do an end-to-end validation of the system/s to ensure it is ready for deploying our databases.		
c)	Placement	The solution shall be offered behind our data center firewalls to meet data sovereignty, security & governance requirements.		
d)	Workload Types	The solution shall have the flexibility to be used as a database platform for the following workloads: OLTP Cloud Data Warehouse In-memory Analytics In-database Machine Learning Database Consolidation		
e)	Infrastructure Management	The solution shall offer our IT staff with a self-service, & with no infrastructure management which shall further reduce our administrative costs by eliminating system management completely.		
f)	Bandwidth & Latency	The solution shall be offered with minimum 100Gbps active-active internal network fabric for providing more bandwidth & least latency.		
g)	High Availability	The solution shall be offered with high-availability. All necessary hardware & software required to achieve the same shall be provided.		
h)	Control Plane	The solution shall be offered with a Control Plane. The Control Plane software shall be installed on minimum 2 Servers to host the secure tunnel endpoint & act as a gateway for access		

SI#	Category	Functional Requirements	Compl ied (Y/N)	Reference
		to the infrastructure. It should also host components that orchestrate the cloud automation, aggregate & route telemetry messages from the environment to the OEM Support Center. Our IT staff shall be able to manage the solution & perform life cycle management operations for our databases running on the platform using this Control Plane. Our IT staff shall be able to connect to the Control Plane through a secure link using a web browser, command line interface (CLI), or REST APIs & perform activities like: User administration, create / modify / delete VM clusters & databases, backup, restore, patching, auditing, track our usage & bill, CPU scaling etc.		
i)	Identity Management	The solution shall be offered with a sophisticated identity management system which shall allow multiple departments or groups to share a tenancy. Policies shall be used to grant fine grain permissions within a single database for separation of duty. For example, one administrator could be responsible for backup & another for patching.		
j)	Backup	The solution shall offer automatic built-in database backup facilities, with weekly full backups & daily incremental backups. Copy 1 shall be on the local disk & Copy 2 shall be in the Object Storage service in the public cloud of the same OEM. In-case the bidder plans to offer an On-prem backup solution then 3 copies are required with a reputed backup software. Copy 1 shall be on Disk Appliance. Copy 2 & 3 shall be on FC		

Sl#	Category	Functional Requirements	Complied (Y/N)	Reference
		based Tape Library. On a weekly basis the set of tapes for Copy 3 shall be vaulted in a secure location in a different seismic zone.		
k)	Security			
1.		The security features of the solution shall segregate our data access & OEM operations & ensure that data that enters or leaves is secure, data that resides on the system is secure, access to the system is secure & the code that runs on the system is secure.		
2.		The solution shall offer automation to further enhance security by enforcing strong passwords & data encryption on all databases & making it fast & easy for us to keep databases updated with the latest security patches.		
3.		The systems offered in the solution shall have vendor signed firmware on most hardware components to ensure hardware components will only run valid code from the vendor that supplied that component.		
4.		The solution shall offer Hardware acceleration that delivers near-native encryption & decryption speed so that encryption can always be used for all database data. The decryption processing shall be done at the storage tier only. In-case decryption is done at the compute tier min 30% additional resources shall be provided.		
5.		The solution shall be designed with minimal open ports & running services that minimize attack surfaces.		
6.		The solution shall offer token-based SSH that provides secure access to our virtual machines.		
7.		The solution shall offer comprehensive logging & auditing that tracks access & modification.		
8.		The solution shall be offered with minimal Linux distribution which ensures that just the packages needed to run Databases are installed & enabled.		
l)	Features			
1.		The solution shall be horizontally scalable.		

Sl#	Category	Functional Requirements	Comp lied (Y/N)	Reference
2.		The solution shall offload data intensive SQL operations to the storage tier. In-case SQL operations are done at the compute tier min 30% additional resources shall be provided.		
3.		The solution shall be offered with persistent memory with low latency.		
4.		The solution shall offer Accelerators to write commit records to persistent memory providing faster log writes.		
5.		The solution shall make use of Storage Indexes to avoid unnecessary I/O operations by replacing them with a few in-memory lookups.		
6.		The solution shall make use of columnar methods to greatly compress data, enabling tremendous cost-savings & performance improvements due to reduced storage capacity & reduced I/O, especially for analytic workloads.		
7.		The solution shall be able to consolidate multiple databases, a portable collection of schemas, schema objects & non-schema objects which will further improve resource utilization, management & overall security.		
8.		The solution shall be able to optimize both analytics & mixed workload OLTP, delivering outstanding performance for transactions while simultaneously supporting real-time analytics, business intelligence & reports.		
9.		The solution shall allow us to run a single Database across multiple servers in order to maximize availability & enable horizontal scalability, while accessing shared storage. User sessions connecting to the Database can failover & safely replay changes during outages, without any changes to end user applications, hiding the impact of the outages from end users.		
10.		The solution shall Ensure high availability, data protection & disaster recovery for our enterprise data. It shall survive disasters & data corruption while creating, maintaining & managing one or more synchronized standby databases. Queries & reports shall be offloaded from the production system to a synchronized physical standby database.		

SI#	Category	Functional Requirements	Comp lied (Y/N)	Reference
11.		The solution shall allow tables, indexes & index-organized tables to be subdivided into smaller pieces, enabling these database objects to be managed & accessed at a finer level of granularity.		
12.		The solution shall offer a comprehensive set of compression capabilities to help improve database performance & reduce storage costs. It shall allow us to reduce our overall database storage footprint by enabling compression for all types of data: relational (table), unstructured (file), index, network & backup data.		
13.		The solution shall offer security option for the database & shall mediate access to data rows by comparing labels attached to data rows in application tables (sensitivity labels) & a set of user labels (clearance labels).		
14.		The solution shall offer data security controls to restrict access to application data by privileged users. It shall reduce the risk of insider & outside threats & address compliance requirements, including separation of duties.		
15.		The solution shall be able to Encrypt application tablespaces to prevent out-of-band access to sensitive data. Redaction policies shall be able to prevent the proliferation of sensitive data & aid in compliance with data protection regulations.		
16.		The solution shall offer Transparent Data Encryption (TDE) which stops would-be attackers from bypassing the database & reading sensitive information directly from storage by enforcing data-at-rest encryption in the database layer. It shall Encrypt individual data columns, entire tablespaces, database exports & backups to control access to sensitive data.		
17.		System changes, such as hardware & software upgrades, configuration changes, etc., are essential for businesses to maintain their competitive edge as well as for compliance & security purposes. The solution shall help us fully assess the effect of such system changes on real-world applications in test environments before deploying the change in production.		
18.		The solution shall allowing developers & analysts to get started easily with location intelligence analytics & mapping		

SI#	Category	Functional Requirements	Complied (Y/N)	Reference
		services. It should enable Geographic Information System (GIS) professionals to successfully deploy advanced geospatial applications.		
19.		The solution shall help Analysts & developers to perform fraud detection, find connections & link to data & improve traceability in smart manufacturing, all while gaining enterprise-grade security, ease of data ingestion & strong support for data workloads.		
20.		The solution shall offer simplified storage management that is consistent across all server & storage platforms & providing the following functionalities: Simplified & automatic storage management. Increase storage utilization & agility. Deliver predictable performance, availability & scalability. Support database failure in the event of server crash.		
21.		The solution shall empower data & business analysts to extract knowledge, discover new insights & make predictions—working directly with large data volumes in the Database. The solution shall offers a combination of powerful in-database algorithms & open source R algorithms, accessible via SQL & R languages & provides a range of GUI & IDE options targeting the spectrum from business users to data scientists.		
m)	Scaling	The solution shall allow us to easily scale our system as business conditions change. We shall be able to scale CPU, memory, local disk space & storage allocated to the VMs from the unified web based console. This will avoid the costly practice of sizing for the highest possible peak workload, which is often required for on-premises systems & with reserved cloud capacity solutions common to the cloud providers.		
n)	Performance Range	The solution shall be designed in a manner of deliver performance within the following ranges as it scales: Physical cores to run database - Min		

Sl#	Category	Functional Requirements	Complied (Y/N)	Reference
		<p>120 - 480. RAM (TB) - Min 2.5TB - 10TB. Physical cores to run storage operations - Min 120 - 480. Flash capacity (TB) - 70TB - 280TB. Backup solution shall be designed Min 10TB. SQL Flash Read IOPS - Min 4.5 Mn - 21.0 Mn. SQL Flash Write IOPS - Min 1.5 Mn - 7.0 Mn. Usable disk space - Min 190TB - 760 TB The bidder to offer the solution with the minimum values in Day 1 & ensure scalability to the maximum values as & when required. Each database server in the solution shall be configured with 4 x 10/25 Gb SFP28 (Fiber) Ethernet, or 4 x 10 Gb RJ45 (Copper) Ethernet.</p>		
o)	Service Level Objective	The offered solution shall provide a Service Level Objective of 99.95%.		
p)	OEM Responsibility	The OEM of the offered solution shall be responsible for the following activities:		
q)	Database Server Hardware	Hardware shipment & Installation Monitor (e.g. Hardware faults) Identification & resolution of issues Incident Management Change Management		
r)	Database Server Hosts	Software Installation & Initial Configuration Monitor Upgrades (e.g. major Software Updates) Updates (e.g. minor Software Updates) OS Security & other Patches Backup/Restore (OS) Identification & resolution of issues		

Sl#	Category	Functional Requirements	Compl ied (Y/N)	Reference
		Tune Incident Management Change Management Firmware updates		
s)	Virtual Machines	Initial Software Installation & Initial Configuration		
t)	Storage Hardware	Hardware shipment & Installation Monitor (e.g. Hardware faults) Identification & resolution of issues Incident Management Change Management Faulty parts replacements (e.g. disks, flash cards etc) Firmware updates		
u)	Storage Software	Software Installation & Initial Configuration Monitor Upgrades (e.g. major Software Updates) Updates (e.g. minor Software Updates) OS Security & other Patches Identification & resolution of issues Incident Management Change Management Tune		
v)	Networking (Fabric & Management switches) & PDU	Hardware shipment & Installation Monitor (e.g. Hardware faults) Identification & resolution of issues Incident Management Change Management Firmware updates		
w)	Hardware Refresh	The systems offered in the solution shall be refreshed by the OEM at the end of 48 months.		
x)	Operating System Support	The OEM shall offer the following support for the Operating System: 24x7 telephone & online support Around-the-clock access to		

SI#	Category	Functional Requirements	Completed (Y/N)	Reference
		<p>enhancements, updates & errata Linux Management Spacewalk support High availability with Cluster ware Comprehensive tracing Linux load balancer</p> <p>Comprehensive indemnification Container runtime for Docker Linux Virtualization Manager Zero-downtime patching Linux Automation Manager/Engine Linux high availability services support</p>		
y)	Managed Service Provided SoW			
<p>The MSP shall work with the OEM in a synchronized manner during the phases of delivery & installation of the infrastructure.</p> <p>Architecture Design: Networking Solution architecture for Prod & Non-Prod. Understand the team's role and responsibilities to manage & design/update the compartments & policies Create & setup of base services such as, Compartments, Administrative Users & Groups, Subnets, Security Lists, Routing Tables, Rules, Policies, etc. IPSec VPN Provisioning. Dedicated connectivity may also be considered for uninterrupted monitoring, administration, trouble shooting and incident management purposes. Provision of the database consolidation platform with required shape & storage as per our requirement. Configure Auto Backup with required retention. Migration of existing databases to the database consolidation platform. Suggesting necessary changes in the application tier so that the applications can communicate with the databases in the database consolidation platform.</p>				

3.11.4 Bill of Material of ORACLE License available with OCAC

SI#	Oracle licenses	Qty
a)	Oracle Database Enterprise Edition	22
b)	Oracle Real Application Clusters	18
c)	Oracle Diagnostics Pack	12
d)	Oracle Tuning Pack	12
e)	Oracle Multitenant	12
f)	Oracle Advanced Security – PII	12

g)	Oracle Audit Vault and Database Firewall	12
h)	Oracle Partitioning	18

(OCAC is free to deploy additional Oracle database license to accommodate other applications as and when required within the limit of the Oracle EXaCC supplied by SI as per the BoQ of this RFP)